ENSURING EFFECTIVE AND RELIABLE ALERTS AND WARNINGS

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

FEBRUARY 6, 2018

Serial No. 115–48

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
30–482 PDF WASHINGTON : 2018

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
JOHN H. RUTHERFORD, Florida
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
DON BACON, Nebraska
BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
STEVEN S. GIAIER, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

DANIEL M. DONOVAN, JR., New York, *Chairman*

PETER T. KING, New York
MARTHA MCSALLY, Arizona
JOHN H. RUTHERFORD, Florida
THOMAS A. GARRETT, JR., Virginia
MICHAEL T. MCCAUL, Texas *(ex officio)*
DONALD M. PAYNE, JR., New Jersey
JAMES R. LANGEVIN, Rhode Island
BONNIE WATSON COLEMAN, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KERRY A. KINIRONS, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director/Counsel*

CONTENTS

ENSURING EFFECTIVE AND RELIABLE ALERTS AND WARNINGS

Tuesday, February 6, 2018

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
RESPONSE, AND COMMUNICATIONS,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:02 a.m., in room HVC–210, Capitol Visitor Center, Hon. Daniel Donovan [Chairman of the subcommittee] presiding.

Present: Representatives Donovan, Payne, and Langevin.

Also present: Representative Jackson Lee.

Mr. DONOVAN. The Subcommittee on Emergency Preparedness, Response, and Communications will come to order. The subcommittee is meeting today to review our ability to timely and effectively alert and warn the public in the case of an emergency. I want to welcome all witnesses here this morning on an issue that is vital to the protection of Americans—effective and reliable alerts and warnings.

The numerous disasters and terrorist attacks that we have witnessed over the past few months, have illustrated that timely communication is critical in an emergency situation, and the availability of critical information can help individuals protect themselves from harm's way.

While some of us grew up in emergency alerts warnings through television, radio, and I am old enough to remember when they told us to get underneath our desks because there was a siren warning, many alerts today are also received through mobile devices, the internet, and even social media.

Considering the technology advances that have been made over the past decade, we have high expectations for what our phones, tablets, and computers can do. At the very least, we expect that the alerts that come through our devices are timely, accurate, and only sent when necessary.

During the Chelsea bombing in 2016, the New York City Emergency Management Department sent out three messages to the Chelsea neighborhood: One to alert individuals to shelter in place; No. 2, once the situation was cleared; and the third one, to solicit the public's help in locating the suspect.

These messages helped protect individuals at a time of uncertainty. It was also reported that they were received far outside the target area.

While it is difficult to obtain 100 percent accuracy, I am glad that the FCC voted last week to require the delivery of alerts to 100 percent of the target area identified by the alert system with no more than one-tenth of a mile overshoot. This kind of accuracy will help to deter warning fatigue.

Unfortunately, there have been erroneous emergency alerts sent to the public that undermines the confidence in the system and the messages that are shared. We saw an example of this just this morning, when an alert that was supposed to be a test, instead warned multiple locations on the East Coast that a tsunami was on its way.

In addition, the erroneous emergency alert issued by the State of Hawaii on January 13, 2018, warning residents and visitors of a ballistic missile threat inbound to Hawaii, has caused the same concern of ours. Because this incident occurred due to human error, I am interested in hearing about the training, certification to message or originators to ensure proper use of the system.

In addition, I am interested in knowing more about the safeguards that should have been in place, and what, if anything, needs to be done on a Federal level to make sure that this never happens again.

In addition, to improve the response to terrorist events, I encourage the FCC to take action on multimedia alerts. Many, too, want feedback and multilingual messaging to further the effectiveness of alerts and warnings.

For example, if New York City Emergency Management was able to send a picture of the suspect directly to recipients' phones during the Chelsea bombing, or if recipients were able to respond to the message to report that they saw the Chelsea bomber, it may have led to a faster apprehension of the suspect.

However, enhancements to the system will be meaningless if basic awareness of how to use the system is not met. Considering the current threat environment in the United States, evidenced by many incidents over the past few months, including two terrorist attacks in New York City, one in October and the other in December 2017, the accuracy and efficiency of wireless emergency alerts is critical. That way, when an eminent threat alert is sent, Americans can and will act accordingly to protect themselves and their loved ones.

I want to thank our witnesses for being here today to share their expertise with us, and I look forward to our discussion.

The Chair now recognizes my friend, the Ranking Member of this subcommittee, the gentleman from New Jersey, Mr. Payne, for an opening statement that he may have.

[The statement of Chairman Donovan follows:]

STATEMENT OF CHAIRMAN DANIEL M. DONOVAN

FEBRUARY 6, 2018

I want to welcome our witnesses here this morning to a hearing on an issue that is vital to the protection of Americans: Effective and reliable alerts and warnings.

The numerous disasters and terrorist attacks that we witnessed over the past few months have illustrated that timely communication is crucial in an emergency situation, and the availability of critical information can help individuals protect themselves from harm's way.

While some of us grew up with emergency alert warnings through television, radio, or even warning sirens, many alerts today are also received through mobile devices, the internet, and social media.

Considering the technological advances that have been made over the past decade, we have high expectations for what our phones, tablets, and computers can do. At the very least, we expect that the alerts that come through on our devices are timely, accurate, and only sent when necessary.

During the Chelsea bombing in 2016, the New York City Emergency Management Department sent out three messages to the Chelsea neighborhood to alert individuals to shelter in place, once the situation was cleared, and to solicit the public's help in locating the suspect.

While these messages helped to protect individuals in a time of uncertainty, it was also reported that they were received far outside the target area. Although I understand that it is difficult to obtain 100 percent accuracy, I am glad that the FCC voted last week to require the delivery of alerts to 100 percent of the target area identified by the alert originator with no more than 1/10th of a mile overshoot. This kind of accuracy will help to deter warning fatigue.

Unfortunately, there have been erroneous emergency alerts sent to the public that undermines confidence in the system and the messages that are shared. We saw an example just this morning when an alert that was supposed to be a test instead warned multiple locations on the East Coast that a tsunami was on its way.

In addition, there was the erroneous emergency alert issued by the State of Hawaii on January 13, 2018, warning residents and visitors of a "Ballistic Missile Threat Inbound to Hawaii." I am very concerned that this will result in a lack of response to actual events and could cause individuals to opt out of receiving lifesaving messages entirely.

Because this incident occurred due to human error, I am interested in hearing more about the training and certification for message originators to ensure proper use of the system. In addition, I am interested to know more about the safeguards that should have been in place, and what, if anything, needs to be done at a Federal level to make sure that this never happens again.

In addition, to improve the response to terrorist events, I encourage the FCC to take action on multimedia alerts, "many to one" feedback, and multilingual messaging to further the effectiveness of alerts and warnings. For example, if New York City Emergency Management was able to send out a picture of the suspect directly to recipients' phones during the Chelsea bombing, or if recipients were able to respond to the message to report that they saw the Chelsea bombing suspect, it may have led to a faster apprehension of a terrorist. However, enhancements to the system will be meaningless if basic awareness of how to use the system is not met.

Considering the current threat environment in the United States evidenced by many incidents over the past few months, including two terrorist attacks in New York City in October and December 2017, the accuracy and efficiency of WEA is critical. That way, when an imminent threat alert is sent, Americans can and will act accordingly to protect themselves and their loved ones.

I want to thank the witnesses for being here today. I look forward to our discussion.

Mr. PAYNE. Good morning, and I would like to thank the Chairman Donovan for holding today's hearing to assess the state of our Nation's alert and warnings systems.

Our ability to issue timely emergency alerts and warnings is an essential component of the National preparedness. We know when the public is warned early and given enough time to protect themselves and their property, we can limit the human toll and mitigate damage to our communities.

Since the Federal Government began pursuing a National alert capability over 50 years ago, we have leveraged advances in technology to push alerts out to a larger population for the public more quickly. At the same time, the Federal Government has undertaken efforts to educate the public about alerts, warnings, and how important it is to respond to them.

Ultimately, for the public alerts and the warnings to be effective, the public has to be able to trust them. This is why last month's false ballistic missile alert in Hawaii was so troubling. I am con-

cerned that a single employee was able to issue an alert in the first place, and that it took nearly 40 minutes to issue a false alarm message over their platform.

That said, false alerts are not limited to Hawaii. During a routine test of the emergency alert system last month, a false alert announcing an emergency in Mars County, New Jersey interrupted programming for certain cable subscribers last month. After Hurricane Irma in Florida last year, an alert issued in error by a State employee directed residents to boil their water, causing hours of confusion.

What these incidents have taught us is that we need enhanced trained and guidance for State and local governments that are authorized to issue emergency alerts through FEMA's Integrated Public Alert Warning System, or IPAWS.

False alerting can be very dangerous, as it can lead to alert apathy, confusion, and unnecessary panic. Nevertheless, we should not allow these incidents to cloud the success of otherwise trustworthy emergency alert and warning systems.

Wireless emergency alerts have been partially effective in keeping people out of harm's way where they are used to warn of inclement weather or a man-made attack.

To date, 33,000 wireless emergency alerts messages have been disseminated. The majority of these messages have been weather-related and were instrumental in saving lives during last year's unusually active hurricane season and unprecedented wildfires.

But it is important to note that the wireless emergency alerts were also sent after the Boston Marathon Bombing and the Chelsea bombing in New York to help law enforcement catch the terror suspects.

As we evaluate the existing alerts and warning systems, I would be interested to learn what efforts are under way at the Federal, State, and local level, to integrate emerging technologies into alerts and warnings procedures.

I look forward to engaging both panels about what has been working well with IPAWS and to gauge where improvement is needed. With that, I thank the witnesses for being here today, and I look forward to your testimony.

I yield back the balance of my time.

[The statement of Ranking Member Payne follows:]

STATEMENT OF RANKING MEMBER DONALD M. PAYNE

FEBRUARY 6, 2018

Good morning. I want to thank Chairman Donovan for holding today's hearing to assess the state of our Nation's alert and warning systems.

Our ability to issue timely emergency alerts and warnings is an essential component of National preparedness. We know when the public is warned early, and given enough time to protect themselves and their property, we can limit the human toll and mitigate damage to our communities.

Since the Federal Government began pursuing a National alerting capability over 50 years ago, we have leveraged advances in technology to push alerts out to a larger population of the public more quickly. At the same time, the Federal Government has undertaken efforts to educate the public about alerts and warnings, and how important it is to respond to them.

Ultimately, for public alerts and warnings to be effective, the public has to trust them. This is why last month's false ballistic missile alert in Hawaii was so troubling. I am concerned that a single employee was able to issue the alert in the first

place, and that it took nearly 40 minutes to issue a "false alarm" message over the platform.

That said, false alerts are not limited to Hawaii. During a routine test of the emergency alert system last month, a false alert announcing an "emergency" in Morris County, New Jersey, interrupted programming for certain cable subscribers last month. After Hurricane Irma hit Florida last year, an alert issued in error by a State employee directed residents to boil their water, causing hours of confusion.

What these incidents have taught us is that we need enhanced training and guidance for the State and local governments that are authorized to issue emergency alerts through FEMA's Integrated Public Alert Warning System or "IPAWS". False alerting can be very dangerous, as it can lead to alert apathy, confusion, or unnecessary panic.

Nevertheless, we should not allow these incident to cloud the success of otherwise trustworthy emergency alert and warning system.

Wireless Emergency Alerts have been particularly effective in keeping people out of harm's way, whether used to warn of inclement weather or a man-made attack. To date, 33,000 Wireless Emergency Alerts messages have been disseminated. The majority of these messages have been weather-related, and were instrumental in saving lives during last year's unusually active hurricane season and unprecedented wildfires.

But it is important to note that Wireless Emergency Alerts were also sent after the Boston Marathon bombing and the Chelsea bombing in New York to help law enforcement catch terror suspects.

As we evaluate the existing alerts and warnings system, I will be interested to learn what efforts are underway at the Federal, State, and local level to integrate emerging technologies into alerts and warnings procedures.

I look forward to engaging both panels about what has been working well with IPAWS, and to gauge what needs improvement.

With that, I thank the witnesses for being here today, and I look forward to their testimony.

Mr. DONOVAN. The gentleman yields. Other Members of the subcommittee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

FEBRUARY 6, 2018

Good morning. I want to thank Chairman Donovan and Ranking Member Payne, Jr. for their on-going to commitment to improving National preparedness and ensuring that our constituents have the information they need to stay safe when disaster strikes.

When Hurricane Katrina struck the Gulf Coast in 2005, we saw first-hand how the lack of a modern National emergency alert capability complicated the immediate response and recovery in the gulf States.

Within a year of the storm, President Bush directed FEMA to accelerate the integration of modernize the aging Emergency Alerts System and leverage new technologies into its alerts and warnings platform, the Integrated Public Alerts and Warnings System (IPAWS).

In the years since, IPAWS has evolved, pushing out alerts and warnings via televisions, radios, and cell phones. IPAWS is exploring opportunities to integrate new technologies, including networked devices.

The program has increased the number of approved alert originators to ensure that State and local governments have the ability to properly issue warnings in their areas.

Toward that end: Emergency alerts and warnings save lives, but only if the public responds to them.

That means the alerts must be accessible to those with access and functional needs, available to those in urban and rural areas alike, and accurate so the public will heed the instruction.

In the past, I have raised concerns about whether alerts and warnings are accessible to people with hearing or vision impairments, as well as those who do not speak English.

I understand that lessons learned from previous tests of the Emergency Alert System have informed updates to the alerting system to make messages clearer for those with limited vision.

I also understand that the IPAWS platform is currently capable of pushing out alerts and warnings in Spanish, and I am interested in learning whether that capability is being utilized and what efforts FEMA is undertaking to broaden the accessibility for those who cannot read or speak English or Spanish.

Moreover, to ensure that emergency alerts and warnings are available to those who live beyond the reach of a cell tower, FEMA must continue to pursue novel approaches to alerts and warnings to reach those who are not watching TV or listening to the radio.

Finally, alerts and warnings must be accurate.

Last month's disturbing false alert about an incoming missile in Hawaii revealed gaps related to training, policy, and procedure for issuing alerts and warnings.

I am not raising this issue to chase a headline or to shame the Federal or State agencies involved.

Rather, I raise this issue because I am concerned that false alerts like the one issued last month could result in the public taking alerts and warnings less seriously, delaying response, or ignoring them all together.

Every minute matters during a disaster, and we cannot afford to have the public wasting time questioning whether an alert is real before taking action.

I look forward to learning how FEMA is updating its training, policies, and best practices to prevent additional false alerts in the future.

With that, I thank the witnesses for being here today and I yield back the balance of my time.

Mr. DONOVAN. We are pleased to have two very distinguished panels before us today on this important topic.

On our first panel, Mr. Antwane Johnson serves as the director of Continuity Communications at the Federal Emergency Management Agency. In this capacity, he oversees the Integrated Public Alert and Warning System.

Ms. Lisa Fowlkes serves as the chief of the Federal Communications Commission's Public Safety and Homeland Security Bureau. In this capacity, she manages the commission's responsibilities related to alerts and warnings, 9–1–1 systems and public safety communications.

The witnesses' full written statements will appear on the record.

The Chair now recognizes Mr. Johnson for his 5-minute opening statement.

STATEMENT OF ANTWANE JOHNSON, DIRECTOR OF CONTINUITY COMMUNICATIONS, FEDERAL EMERGENCY MANAGEMENT AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. JOHNSON. Thank you, Chairman Donovan, Ranking Member Payne, and Members of the subcommittee. My name, as mentioned, is Antwane Johnson, and I am the director of Continuity Commutations at FEMA. On behalf of Secretary Nielson and Administrator Long, thank you for the opportunity to discuss the Integrated Public Alert and Warning System, also known as IPAWS, and how it is used to save lives across the country.

An effective and timely public alert and warning system is critical to communicating threats to the public, providing people with guidance during times of crisis.

At FEMA we manage IPAWS and its two main components: Warnings and communications from the President in the event of a catastrophic National emergency through the National Public Warning System; and we manage geo-targeted alerts sent from Federal, State, local, and Tribal officials during emergencies such as those issued last year during hurricanes and wildfires.

IPAWS allows those alerting authorities to send emergency messages to people in their geographic jurisdiction by emergency alert system broadcast through radio and TV, wireless emergency alerts to cell phones, broadcast from NOAA weather radios and other internet-connected services.

Today, IPAWS supports more than 1,000 Federal, State, local, Tribal, and territorial users, more than 26,000 radio, TV, and cable connections, 63 cellular carriers' gateways reaching millions of cell phones, connections to NOAA dissemination systems, 73 internet vendors that tap into the alert feed.

We established a connection between IPAWS and Canada's multi-agency situational awareness system for the exchange of disaster information between our countries.

Since inception of the system in 2012, there have been nearly 3 million messages disseminated throughout IPAWS. These messages, which cover everything from a natural disaster or an active shooter, to missing children and planned power outages, help communicate critical life-saving information to the public.

For example, after a camp manager in Windsor, Connecticut received a wireless emergency alert on her mobile device, she evacuated 29 children from a soccer dome just before an EF1 tornado touched down and ripped the roof off.

In 2016, New York City sent a wireless emergency alert with an electronic wanted poster to identify a suspect in connection with bombings in Manhattan and New Jersey. The suspect was captured within hours.

Last year, wireless emergency alerts were used by officials to issue warnings and evacuation orders in Texas, Florida, and California in response to hurricanes and wildfires.

Significantly since 2012, 47 kidnapped children have been returned to their loved ones after an Amber Alert was issued through the system. Members of the community help law enforcement locate perpetrators.

In addition to managing the IPAWS program, FEMA helps train users and create guidance for alerting authorities and software tool vendors.

It is important to note that while FEMA manages the IPAWS system, we rely on our State and local partners to originate communications to their jurisdictions, as they are the boots on the ground that are best able to communicate the threats they face and provide specific protective action information related to their area.

Following direction from Congress and the IPAWS Modernization Act of 2015, FEMA has established a subcommittee to the National Advisory Council.

The subcommittee includes members from State, local, Tribal, and territorial governments, communication service providers, organizations representing individuals with access and functional needs or limited English proficiency and others. This subcommittee is consulting with IPAWS users and experts to consider new and developing technologies that may be beneficial to IPAWS and the Nation.

The subcommittee will develop recommendations on matters related to common alert and warning protocols, standards, terminology, and operating procedures. Through this subcommittee we

are looking at recent uses of the system, including use during the 2017 natural disasters, as well as the false alert in Hawaii, to identify lessons learned.

In addition to this holistic review, there are some key areas in which the IPAWS program is focused for the future. First, we have been engaging vendors of IPAWS-compatible software to encourage better integration of IPAWS screens for consistency and creating of effective alert and warning messages.

In collaboration with the partners, we are continuing to promote adoption and use of IPAWS by public safety officials. We make sure that State, local, Tribal, and Government officials are aware of our IPAWS lab for testing, to ensure they can maintain proficiency and understand the proper use of the system.

I look forward to continuing to work with Congress and provide updates as we move forward with recommendations to continue to modernize the system and our procedures.

I am grateful for the opportunity to appear before you today, and I am happy to respond to any questions this subcommittee may have at this time. Thank you.

[The prepared statement of Mr. Johnson follows:]

PREPARED STATEMENT OF ANTWANE JOHNSON

FEBRUARY 6, 2018

INTRODUCTION

Good morning Chairman Donovan, Ranking Member Payne, and Members of the committee. My name is Antwane Johnson, and I am the director of continuity communications within the National Continuity Programs Directorate (NCP) at the Federal Emergency Management Agency (FEMA). On behalf of FEMA Administrator Brock Long and John Veatch, the assistant administrator for NCP, I appreciate the opportunity to speak today on the importance of the Integrated Public Alert and Warning System (IPAWS), how it is used to save lives across the country, and the future of the IPAWS program.

WHAT IS IPAWS?

An effective, timely, and far-reaching public alert and warning system is critical to communicating threats to public safety and providing people with guidance during times of crisis.

Executive Order 13407 and *The IPAWS Modernization Act of 2015* define FEMA's responsibility to provide a public alert and warning system. *Section 706 of the Communications Act of 1934* requires Presidential access to commercial communications during "a state of public peril or disaster or other National emergency." *The Robert T. Stafford Disaster Relief and Emergency Assistance Act* directs FEMA to provide technical assistance to State, local, Tribal, and territorial (SLTT) governments to ensure that timely and effective disaster warning is provided. In accordance with these statutes, IPAWS was created to enhance and extend a National infrastructure and capability to SLTT officials for public alert and warning.

IPAWS is a National system for local alerting. There are two main system components:

(1) IPAWS supports warnings and communications from the President in the event of a catastrophic National emergency. The President can reach the American people through the National Public Warning System, where the message is transmitted through FEMA Primary Entry Point (PEP) radio stations and Emergency Alert System (EAS) radio, television, and cable stations.

(2) IPAWS also supports geo-targeted alerts sent from Federal and SLTT officials during emergencies, such as those issued last year by Florida and Texas, in anticipation of Hurricanes Harvey, and Irma.

These Federal and SLTT alerting authorities can, via the "IPAWS OPEN" gateway, send emergency messages to people in their geographic jurisdiction by radio and TV Emergency Alert System (EAS) broadcasts, Wireless Emergency Alerts (WEA) to cell phones, broadcasts from National Oceanic and Atmospheric Adminis-

tration (NOAA) Weather Radios, and other IPAWS internet-connected services. The DHS Science and Technology Directorate (S&T) conducted research to improve geo-targeting capabilities and public response to alerts and warnings, through funding provided by the Department of Commerce's National Telecommunications and Information Administration. Today, IPAWS supports more than 26,000 radio, TV, and cable EAS connections, 63 cellular carrier gateways reaching millions of cell phones, connections to NOAA dissemination systems, and 73 internet application vendors that tap into the IPAWS alert feed.

States determine who their State alerting authorities are, and validate requests from potential local alerting authorities to gain access to the IPAWS. A profile is created in the system for each validated authority describing the geographic jurisdiction, types of alerts, and which alert dissemination systems will be used by the authority. Following completion of required FEMA-developed training by the authority, access to send alerts directly through IPAWS to people is turned on. This training provides skills to draft effective and accessible warning messages, and best practices in effective use of the Common Alerting Protocol. In addition to the initial training, in June 2014 FEMA released an advanced course to further develop these skills among alerting authorities. Messages that match the authorities profile pass automatically through the system to EAS, WEA, and the other alert dissemination systems to TV, radio, and cell phones.

IPAWS supports "broadcast" type alert and warning services. Unlike subscription based-alert services, warnings are sent to all people located in a specified area, both residents and visitors.

FEMA is responsible for development, operation, integration, and maintenance of IPAWS infrastructure, which includes the EAS, WEA, NOAA, and IPAWS Alerts Feed components plus any future connections. IPAWS was designed so it can easily adapt to technological advances.

As of January 2018, there are 1,026 total IPAWS public alerting authorities. Since its inception in 2011, more than 2.7 million alert messages have been processed by IPAWS.

Authorities have used IPAWS connections to successfully alert people of a wide variety of threats to public safety. This includes, but is not limited to: Natural disasters, gas plant explosions and evacuations, armed robbers, active shooters, dangerous water advisories, 9–1–1 service outages, and electrical power outages.

AMBER ALERTS

In 2003, President George W. Bush signed the *Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act of 2003* (Public Law 108–21). This Act established the National coordination of State and local programs, including the development of guidance for issuance and dissemination of AMBER alerts.

The National Center for Missing & Exploited Children (NCMEC) is responsible for America's Missing: Broadcast Emergency Response (AMBER) plan, which allows broadcasters and transportation authorities to immediately distribute information about recent child abductions to the public and enables the entire community to assist in the search for and safe recovery of the child.

The AMBER Alert program is a voluntary partnership among law enforcement agencies, broadcasters, transportation agencies, and the wireless industry to activate an urgent Wireless Emergency Alert in the most serious cases of child abduction.

Since the AMBER alert program's inception, nearly 50 children across the country have been safely returned to their families as a direct result of these WEAs.

IPAWS USE DURING RECENT HURRICANES, WILDFIRES, AND MUDSLIDES

For the three major hurricanes in 2017—Harvey, Irma, and Maria—nearly 700 emergency messages were sent via IPAWS by both the National Weather Service and State and local alerting authorities.

Prior to Hurricane Irma, State and local alerting authorities issued a series of timely WEA and EAS alerts to advise the public to take appropriate protective measures. The Florida Division of Emergency Management (FDEM) issued several evacuation alerts that facilitated the safe evacuation of nearly 6.5 million residents. FDEM issued IPAWS alerts on behalf of counties that were unable to issue an alert because they were not an authorized alerting authority, demonstrating State-local coordination.

For Hurricane Maria, FEMA IPAWS developed an innovate arrangement with SirusXM to deploy satellite radios to Puerto Rico. Extensive efforts by the IPAWS project management office successfully kept PEP stations broadcasting in Puerto

Rico to provide critical response and recovery information to the island's residents. These efforts included coordination of fueling where power was unavailable, and providing technical assistance to ensure the PEP stations remained up and running. In the U.S. Virgin Islands, FEMA IPAWS had primed the backup generator for the PEP station 2 years ago and had replaced the fuel tank generator and fuel distribution systems in June 2017. This continued maintenance allowed for radio broadcasts and alerts to be sent to residents in the U.S. Virgin Islands through this station while the power was out following Hurricane Irma.

In October 2017, WEAs were issued to warn California residents about the wildfire danger. No fatalities were recorded in counties that issued these alerts, suggesting the warnings may have helped save lives. This event highlighted a few strengths as well as areas for improvement. Strengths include some local authorities using a variety of warning and communications methods to reach as many people as possible, including WEAs, police sirens, opt-in reverse 9–1–1 and text alerts, door-to-door notifications and social media. Areas for improvement include the regular testing of IPAWS to ensure the system, and user access, is operational and working correctly. One alerting authority's user access was recently updated and was not tested prior to attempted use during the wildfires, at which time it was discovered to have not worked. It has since been fixed.

During the January 2018 flooding and mudslides in Southern California, 10 WEAs were sent: Five by the National Weather Service, three by Santa Barbara County, and two by the city of Los Angeles.

IMPLEMENTATION OF IPAWS MODERNIZATION ACT

The IPAWS Modernization Act of 2015 (Pub. L. 114–143) directs FEMA to implement and modernize the IPAWS and to establish an IPAWS subcommittee under the National Advisory Council (NAC). This council advises the administrator on all aspects of emergency management to ensure input from and coordination with State, local, Tribal, and territorial governments, non-profit organizations, and the private-sector communities on the development and revision of plans and strategies.

Additionally, the law directs the IPAWS subcommittee to consult with users and experts to consider new and developing technologies that may be beneficial to the public alert and warning system; develop recommendations for IPAWS and submit a recommendation report to the NAC for approval. The recommendations will be on matters related to common alerting and warning protocols, standards, terminology, and operating procedures. The subcommittee will also make recommendations to the NAC on having the capability to adapt the distribution and content of communications based on locality, risks, or user preferences. As outlined in the law, the subcommittee will terminate no later than April 2019.

FEMA announced the IPAWS subcommittee membership in July 2017. Membership includes participants from: State, local, and Tribal governments and emergency management agencies; communications service providers; third-party service bureaus; commercial mobile radio service industry; satellite industry; organizations representing individuals with access and functional needs and limited English proficiency; privacy advocates; and senior Federal leaders. The subcommittee members are divided into four working groups, focused on: Alert writers and alerting authorities; public needs; stakeholder engagement and coordination; and future technologies.

As of January 2018, the working groups have held 31 webinars, with 39 guest speakers presenting to subcommittee members. These guest speakers include educators and researchers, State and local alerting authorities, and private-sector partners to help inform the recommendations.

The subcommittee will continue developing and refining recommendations in the coming months, in order to present draft recommendations to the NAC in fall 2018. The subcommittee will also take into consideration recent uses, including best practices and lessons learned, when developing the recommendations. Once a draft is complete, the subcommittee will work with the NAC to develop the final approved recommendations to present to the FEMA administrator.

IPAWS PROGRAM GOALS AND CHALLENGES

As the subcommittee recommendations to the NAC are still being developed, there are some key areas in which the IPAWS program is focused for the future.

The IPAWS program office has been engaging vendors of IPAWS-compatible software to encourage better integration of IPAWS screens for consistency and creation of effective public alert and warning messages.

The program will continue to promote adoption and use of IPAWS by emergency management and public safety officials. Through the IPAWS Stakeholder Engage-

ment and Customer Support teams, the program works with State, local, Tribal, and territorial officials to promote use of the system. IPAWS also provides information and support on various Federal grant programs that may be able to provide funding for alerting authorities to purchase alerting software that interfaces with IPAWS.

IPAWS will also continue to make SLTT emergency managers aware of the "IPAWS Lab." This lab, located at the Naval Surface Warfare Center in Indian Head, Maryland, provides alerting authorities with test and evaluation, operational assessments, IPAWS demonstrations, and expert technical support. The lab provides an interactive and closed IPAWS testing environment, and allows users the opportunity to practice and train to increase familiarity and confidence using IPAWS.

In accordance with new WEA rules established by the Federal Communications Commission (FCC) in 2016, IPAWS is working with wireless carriers and alerting software vendors to enhance WEA capabilities based on research conducted by S&T. This includes creating room for more detailed information in messages, allowing links to instructions and images, Spanish language support, and dedicated test message type for use by SLTT alerting authorities.

The IPAWS Program Office continues to collaborate with our alerting authority partners to look for opportunities to incorporate best practices and lessons learned into program guidance and training.

CONCLUSION

Every day I am grateful for the opportunity to work with a program dedicated to helping alert and provide guidance to people during times of crisis. Thank you for your interest in the program and we look forward to collaborating with this subcommittee on ways the program can improve. I am happy to take any questions you have at this time.

Mr. DONOVAN. Thank you, Mr. Johnson.

The Chair now recognizes Ms. Fowlkes for 5 minutes.

STATEMENT OF LISA FOWLKES, CHIEF, PUBLIC SAFETY AND HOMELAND SECURITY BUREAU, U.S. FEDERAL COMMUNICATIONS COMMISSION

Ms. FOWLKES. Good morning, Chairman Donovan, Ranking Member Payne, and Members of the subcommittee. Thank you for the opportunity to appear before you to discuss our Nation's emergency alert systems.

As I recently testified before the U.S. Senate Committee on Commerce, Science, and Transportation, the false ballistic missile warning issues on January 13 by the State of Hawaii was unacceptable. It resulted in wide-spread panic, and the extended period it took to correct the error, nearly 40 minutes, compounded the problem.

Looking beyond the immediate consequences of the mistake, which were serious in and of themselves, this cry of wolf damaged the credibility of alert messaging, which can be dangerous when a real emergency occurs. The commission acted swiftly to open an investigation into the matter. That investigation is on-going, however.

The FCC's Public Safety and Homeland Security Bureau prepared a preliminary report at the commission's January 30 open meeting. I have included the presentation made at the open meeting with my written statement for the record.

But briefly, as the bureau reported, it appears that the false alert was the result of two failures, first, simple human error. Second, the State did not have safeguards or process protocols in place to prevent that human error from resulting in the transmission of a false alert. Moving forward, the commission will focus on ways to prevent this from happening again.

Federal, State, and local officials throughout the country need to work together to identify any vulnerabilities to false alerts and do

what is necessary to fix them. We also must ensure that should a false alert nonetheless occur, a correction is issued promptly in order to minimize confusion.

Emergency alerting systems provide timely and life-saving information to the public, and we must take all measures to bolster and restore the public's confidence in these systems.

The commission is also looking into the recent tsunami alerts issued following the 7.9 magnitude in the Gulf of Alaska on January 23 to better understand how the Wireless Emergency Alert System, or WEA, performed.

While the incidents in Hawaii, and Alaska, and other places are very present in our minds, we cannot lose sight of the fact that wireless emergency alerts have greatly enhanced public safety.

In the last 5 years, WEA has been used to issue over 35,000 emergency alerts. Since WEA was first deployed in 2012, the commission has taken significant steps to enhance alerting capabilities by leveraging advancements in technology.

Just last week, the commission voted to require participating wireless providers to deliver alerts in a more geographically precise manner. Specifically, participating wireless providers must deliver WEA alerts to the target areas specified by the alert originator, with no more than one-tenth of a mile overshoot by November 2019.

This rule will help channel alerts to Americans who actually need them, while reducing over-alerting. Equally important, this rule will give alert originators the assurance they need to rely on WEA as a valuable tool to help save lives.

The recent order also requires that WEA alert messages remain available in a consumer accessible format on wireless devices for 24 hours after receipt, or until the consumer chooses to delete the message. Other enhancements to WEA include Spanish language alerting and increasing the length of alert messages from 90 to 360 characters. These changes will strengthen the WEA system and keep Americans safer.

We also continue to work to advance the integrity and utility of the traditional emergency alert system.

Just this past December, for example, the commission adopted a new blue alert code that will allow State and local officials to notify the public of threats to law enforcement and help apprehend dangerous suspects. Blue alerts may be sent over both the EAS, which delivers warnings to the public via radio and television and WEA.

Over the past several years, the FCC has also worked closely with FEMA to conduct Nation-wide tests of the EAS to assess its reliability and effectiveness. The most recent test was conducted last September, and our initial analysis shows improvements in most areas from the previous year.

In closing, we look forward to partnering with emergency management professionals, industry, and our Federal partners on the alerting capabilities that they need to use America's public alert and warning systems with confidence during times of crisis.

Thank you, and I look forward to any questions you may have.

[The prepared statement of Ms. Fowlkes follows:]

PREPARED STATEMENT OF LISA M. FOWLKES

FEBRUARY 6, 2018

Good morning, Chairman Donovan, Ranking Member Payne, and Members of the subcommittee. Thank you for the opportunity to appear before you to discuss our Nation's emergency alerting systems.

As I recently testified before the U.S. Senate Committee on Commerce, Science, and Transportation, the false alert issued on January 13 by the State of Hawaii, in which recipients were warned of an imminent ballistic missile attack, was absolutely unacceptable. It resulted in wide-spread panic, and the extended period it took to correct the error—nearly 40 minutes—compounded the problem. Looking beyond the immediate consequences of the mistake, which were serious in and of themselves, this cry of "wolf" damaged the credibility of alert messaging, which can be dangerous when a real emergency occurs.

The Commission acted swiftly in the wake of this incident to open an investigation into the matter. That investigation is on-going; however, the Public Safety and Homeland Security Bureau last week presented a preliminary report to the Commissioners at the FCC's January 30 Open Meeting, the presentation materials for which are attached to this written statement. Based on our investigation thus far, the Bureau finds that a combination of human error and inadequate safeguards contributed to this false alert.

While the mistake was realized very quickly, it took 38 minutes for a correction to be issued through the alerting system.

The Hawaii Emergency Management Agency has advised us that it is working with its vendor to integrate additional technical safeguards into its alert origination software, and has changed its protocols to require two individuals to sign off on the transmission of tests and live alerts to ensure that a similar incident does not happen again.

The Commission is also looking into the recent tsunami alerts issued following the 7.9 magnitude earthquake in the Gulf of Alaska on January 23 to better understand how the Wireless Emergency Alert system performed. We are aware that questions have arisen about who received the alerts and who didn't, both with respect to carriers' participation in WEA and with respect to the geographic distribution of the alert, and we will seek answers.

Moving forward, the Commission will focus on what steps need to be taken to prevent an incident like the one in Hawaii from happening again, and will issue a final report at the conclusion of our investigation. Once issued, we will work with FEMA to engage in stakeholder outreach, and encourage the use of best practices. It will also be incumbent upon Federal, State, and local officials to work together to prevent such a false alert from happening again. We also must ensure that corrections are issued immediately after a false alert goes out in order to minimize panic and confusion.

Emergency alerting systems provide timely and life-saving information to the public, and stakeholders must come together to take all necessary measures to bolster and restore the public's confidence in these systems.

The incidents in Hawaii and Alaska are very present in our minds. But I would be remiss in not discussing the benefits of and success stories behind wireless emergency alerts. In this respect, I would like to describe the FCC's efforts to support Wireless Emergency Alerts, commonly known as "WEA," since the system was deployed in April 2012.

To provide you with the scope of its impact, in the last 5 years, WEA has been used to issue over 35,000 emergency alerts. The National Weather Service alone has sent well over 33,000 WEA alerts. For example, we understand that local California officials used WEA 4 times in response to the 2017 wildfires in Northern California, and 16 times for the Los Angeles area wildfires. Representatives from the California Governor's Office of Emergency Services and officials in Marin and Mendocino Counties reported successful use of WEA to move citizens in their jurisdictions to safety. WEA was also used extensively in all areas affected by the 2017 hurricanes, including 21 WEA alerts sent in Puerto Rico alone.

WEA also helps to recover missing children. In 2016 alone, 179 AMBER Alerts were issued in the United States involving 231 children. Since the system was deployed in 2012, WEA has been credited with the safe return of 47 missing children.

The Commission places the highest priority on ensuring that emergency management authorities and first responders have the most up-to-date alerting tools available to them. Since WEA was first deployed in 2012, the Commission has taken significant steps to enhance Federal, State, and local alert and warning capabilities to leverage advancements in technology.

In September 2016, the Commission adopted rules to enable wireless alerts to contain more content by increasing message length from 90 to 360 characters and by supporting embedded phone numbers and URLs. It also took action to enable support for alerts written in Spanish and make it easier for State and local authorities to test WEA, train personnel, and raise public awareness about the service.

The Commission also recognized that it is critical for emergency managers to be able to geographically target alerts to only those phones located in areas affected by an emergency. When the WEA program launched in 2012, participating wireless providers were generally required to send the alerts to a geographic area no larger than the county or counties affected by the emergency situation. As of last November, all participating wireless providers are now required to transmit alerts to a geographic area that best approximates the area affected by the emergency situation, even if it is smaller than a county.

But the Commission did not stop there. Last Tuesday, the Commission voted to require participating wireless providers to target alerts to the impacted area with an overreach of no more than one-tenth of a mile by November 30, 2019. The Commission's recent action also requires that alert messages remain available in a consumer-accessible format on wireless devices for 24 hours after receipt, or until the consumer chooses to delete the message, which will enable the public to better review emergency information. The Commission also adopted enhanced consumer notification requirements at point-of-sale, to ensure consumers understand the benefits of enhanced geo-targeting and the extent to which the wireless provider offers enhanced geo-targeting on its network and devices.

Public safety officials support the Commission's recent action. For example, Francisco Sanchez, Deputy Emergency Management Coordinator at the Harris County, Texas, Office of Homeland Security & Emergency Management stated that the rule changes "set a much needed course to keep the Nation's Wireless Emergency Alerts system a trusted life-saving tool for the public safety community, and is the single greatest improvement in years to the country's alerts and warnings infrastructure," and that it "will empower local public safety officials with the tools necessary to keep WEA relevant and their communities safer."[1]

By matching alerts to phones actually located within the affected area, the Commission's action will assist emergency response efforts and instill confidence in the public's reliance on WEA. Because people will be receiving alerts that are relevant to them, they will be less likely to opt out of the program and more likely to take the alerts they receive seriously. We are also currently considering how to provide emergency managers with the ability to transmit alerts in languages in addition to English and Spanish, alerts that can contain pictures, and alerts that could provide the public with the ability to reply.

While WEA is a powerful alert and warning tool, it is also important to note that it is only one among several tools available to emergency managers to alert and warn their communities.

For example, the Emergency Alert System, or EAS, is the traditional system used to provide alerts and warnings to the public over broadcast, cable, and satellite systems, and remains a vital tool for emergency managers, State, and local authorities. The Commission has been working to modernize the EAS to ensure that it remains a relied upon and useful tool. For example, just this past December the Commission adopted a new "blue alert" code for both EAS and WEA that will allow alert originators to provide targeted information to the public regarding threats to law enforcement and to help apprehend dangerous suspects. In November, the Chairman also circulated an item for the Commission's consideration that would modernize and streamline the filing process for EAS state plans. In addition, last November the FCC authorized the rollout of Next Generation TV, also known as ATSC 3.0, on a voluntary, market-driven basis. Next Gen TV offers a new and improved method to provide consumers with vital information during emergencies. For example, it will enable advanced emergency alerting that could wake up sleeping devices to warn consumers of imminent emergencies. It will also allow for localized, emergency alerts in a variety of languages, and enhanced datacasting to serve law enforcement and first responders more efficiently.

Over the past several years, the FCC has also worked closely with FEMA to conduct Nation-wide tests of the EAS to assess its reliability and effectiveness. The FCC has also successfully deployed the EAS Electronic Reporting System, or ETRS, a user-friendly database that allows the over 25,000 EAS participants to report test results in close to real time. The most recent test was conducted on September 27,

[1] FCC Approves Life-Saving Enhancements to Wireless Emergency Alerts, Public Safety Officials Applaud Step Forward, Press Release (Jan. 30, 2018), at *http://www.readyharris.org/News-Information/Ready-Harris-News/Post/30743?platform=hootsuite*.

2017, and our initial analysis of the ETRS results shows improvements in most areas. For example, results indicate more than 95 percent of participants received the test alerts, and nearly 92 percent successfully retransmitted the alert—both up from the previous year. Further, more than twice as many EAS Participants retransmitted the Spanish language version of the alert than was the case in 2016. In all, we are encouraged by the results and will continue to strive to find ways to enhance the EAS as well.

In closing, we look forward to partnering with emergency management professionals from your jurisdictions on the alerting capabilities that they need to use EAS and WEA with confidence during crises when every second counts.

Thank you for your consideration, and I look forward to any questions you may have.

Federal Communications Commission
Public Safety and Homeland Security Bureau

Preliminary Report:

Hawaii Emergency Management Agency's January 13, 2018 False Ballistic Missile Alert

January 30, 2018

Public Safety & Homeland Security Bureau Status of Investigation

- At 8:07 AM on January 13, 2018, the Hawaii Emergency Management Agency (HI-EMA) issued a false ballistic missile alert through the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA) System. Chairman Pai immediately called on the Bureau to investigate.
- To date, the Bureau has interviewed key stakeholders, including:
  - HI-EMA employees
  - Representatives of other emergency management agencies across the country
  - Alert origination software vendors (including the vendor who supplies HI-EMA)
  - Wireless service providers
- The Bureau's investigation is ongoing.

2

Events Leading Up to the False Alert

Time	Events
0805	• HI-EMA's midnight shift supervisor begins a no-notice ballistic missile defense drill at a shift change by placing a call, pretending to be U.S. Pacific Command, to the day shift warning officers. • The midnight shift supervisor plays a recording over the phone that properly includes the drill language "EXERCISE, EXERCISE, EXERCISE," but also erroneously contains the text of an EAS message for a live ballistic missile alert, including the language, "THIS IS NOT A DRILL." The recording does not follow the script contained in HI-EMA's standard operating procedure for this drill. • The day shift warning officers receive this recorded message on speakerphone. • While other warning officers understand that this is a drill, the warning officer at the alert origination terminal claimed to believe, in a written statement provided to HI-EMA, that this was a real emergency, not a drill.
0807	• This day shift warning officer responds, as trained for a real event, by transmitting a live incoming ballistic missile alert to the State of Hawaii. • In doing so, the day shift warning officer selects the template for a live alert from a drop-down menu, and clicks "yes" in response to a prompt that reads, "Are you sure that you want to send this Alert?"

Events After the False Alert

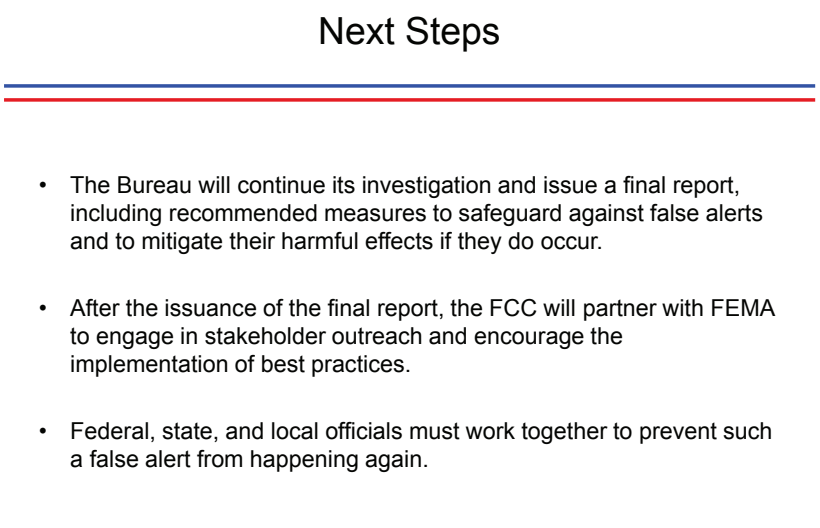
Time	Events
0808	• Day shift warning officer receives false WEA on mobile device
0809	• HI-EMA notifies Hawaii Governor of false alert
0810	• HI-EMA to U.S. Pacific Command and Honolulu PD: no missile launch
0812	• HI-EMA issues a cancellation, ceasing retransmission over EAS, WEA
0813	• HI-EMA begins outreach, but its phone lines become congested
0820	• HI-EMA posts on Facebook, Twitter – “NO missile threat to Hawaii”
0824	• Hawaii Governor retweets notice that there is no missile threat
0827	• HI-EMA determines that an EAS, WEA Civil Emergency Message (CEM) is the best vehicle for correction
0830	• FEMA confirms HI-EMA’s view on CEM; Hawaii Governor posts correction on Facebook
0831	• HI-EMA supervisor logs into alert system, begins to create false alert correction
0845	• HI-EMA issues correction through EAS and WEA that there is no missile threat

Preliminary Findings

1. A combination of human error and inadequate safeguards contributed to the transmission of this false alert.

2. HI-EMA’s lack of preparation for how to respond to the transmission of a false alert was largely responsible for the 38-minute delay in correcting the alert.

3. HI-EMA has taken steps designed to ensure that an incident such as this never happens again.



Mr. DONOVAN. Thank you, Ms. Fowlkes, for your testimony.

I now recognize myself 5 minutes for questions. They are scheduling votes somewhere between 11 o'clock and 11:15, so we are going to try to get through everyone's testimony and allow all our Members.

I ask unanimous consent to have Ms. Jackson Lee from Texas sit on our panel with us. Seeing no objection, welcome, Ms. Jackson Lee.

I have a question for both of you, and in any order of which you would like to speak about it. As I mentioned in my opening statement, it is vital that the public have confidence in our alert system that they receive from their Government, and I fear that the erroneous alert that occurred in Hawaii may erode that trust and lead some people from opting out of the system.

So as you continue to review what happened in Hawaii, do you have any recommendations now? I know your investigation is in its initial stages, but is there any recommendations that you could share with us now after what you have already been able to review on what we could do to prevent that from happening again?

Ms. FOWLKES. At this point, the bureau and the commission have not announced any specific recommendations. As you say, our investigation is on-going, and the plan is once we have completed that investigation, we may have recommendations to share.

Mr. JOHNSON. Thank you, Congressman. From the FEMA perspective, we are conducting an after-action review of the events of January 13. I think there are a number of things that we can do to ensure that the eroded public confidence that has resulted from this mishap on January 13 is improved over time.

One of the things that we can do, and that we are doing, is within FEMA is taking every step that we can take to ensure that this does not happen again.

Second, I think there is the opportunity for us to work with the software tool vendors that provide these applications to State and local governments for their use to improve those tools.

In fact, we have met with and talked to the vendor that provides that software application to the State of Hawaii, as well as 47 other State and local governments. They will be rolling out this week improvements to their system, or their software, to prevent against these types of errors from occurring in the future.

Second, we are revisiting our training to ensure that our training adequately addresses the type of error that took place on January 13 so that emergency management officials are properly prepared to respond to that type of event, even when it is in error.

Then third, we would suggest that there be a broad public information campaign, both on the part of State and local government, to inform citizens of what these technologies are and what they mean to the public when these messages are received.

But we also think there should be a broader over-arching public information campaign, that would include things like testing, exercising to make sure that we include the whole of community in our exercise programs so that the entire community is better prepared to deal with any threat to public safety that they may face.

Mr. DONOVAN. I understand that you haven't completed your investigation. I know some of the recommendations, or the things that we have been reading about, would include not having one person make the determination that this alert should be issued, having the alert be in two different places so even if it is one person they would have time they would have to go to multiple locations to send the alert.

Why the same mechanism of issuing the alert wasn't used in Hawaii to allow the public to know that it was a test, apparently the recalling of the alert wasn't pushed through the same system that sent the alert. It used other mechanisms, such as social media and whatnot. As my friend Don Payne said, it took nearly 40 minutes for that to happen.

There was something I read where people were saying maybe the Federal Government is the only ones that should be allowed to issue such an alert. Could you speak on any of those items here before the committee now?

Mr. JOHNSON. Thank you, Chairman Donovan. I would be happy to speak on those issues. The event of, you know, what took place on January 13 at 8:07 in the morning, was certainly a tragic event.

I think what we are seeing now, as you mentioned the two-factor validation of a message, we have seen that take place in some of the more major cities. In fact, I think the next panel will speak to some of those best practices that are emerging throughout the community.

Those type things, where you have two-factor or two-person validation of a message before it is sent, works in our major cities where their emergency operation centers are well-staffed, and they have the personnel to perform that function.

It doesn't work as well in rural areas where the chief of police in a single office may be the person who is responsible for sending that message to the public and responds to any threat to public safety.

But I do think that where appropriate we will see those type best practices emerge within the community, two-factor authentication, additional software checks or validation checks in the software that is being used by our State and local partners.

I think what we will see in addition to that is better training, a very thorough review of the policies and procedures that are employed to send these messages. FEMA will be prepared to work with our State and local partners in every aspect of that.

In fact, I see that there is a natural progression from the guidance that we issued in 2015 to software vendors, wherein the initial offerings of those tools that we made available to State and local government, for example, did not include a cancel function, although the tool would allow them to originate a message, there was no ability to cancel the message.

So in 2015 we worked with the vendor community and issued recommendations to them on things that they could do to improve their software applications.

We are likewise doing the same thing with the vendor community and looking at other opportunities that they may have to improve their tools to ensure that those type of errors that occurred on January 13 do not occur again.

Mr. DONOVAN. Thank you very much, Mr. Johnson. My time has run out.

Ms. Fowlkes, can you tell me in 15 seconds, you were talking about how we are going to expand the ability and we are going to have multi-lingual alerts. We are going to be able to push out photographs. We have expanded the amount of characters that can be on an alert.

Do we a time frame for those things? Are some of those things in place now, and in the future how long would you see that coming to fruition for us?

Ms. FOWLKES. The rules that the commission adopted regarding the extension of the character limit from 90 to 360, as well as the requirement that participating wireless carriers support Spanish language alerts, would go into effect in May 2019.

The geo-targeting rule that was adopted just last week would go into effect in November 2019. The reason for this is to allow time for the industry to do standards development testing and then whatever upgrades they need to their networks and devices.

Mr. DONOVAN. Thank you very much.

The Chair now recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

Mr. Johnson, you know, in light of the incident in Hawaii, is FEMA considering implementing any additional requirements such as on-going training, multi-person alert verifications or false alert plans? Are the State and local governments seeking to become alert originators as well?

Mr. JOHNSON. Thank you, Ranking Member Payne. With regards to the requirements for a State or local, territorial, or Tribal gov-

ernment to gain access to IPAWS, there are basically four steps that any alerting authority would go through in order to become an alerting authority.

First, they must have a valid software that interfaces with IPAWS, and that software has to meet certain development requirements that we have established with the software tool providers. It has to go through testing and should have demonstrated that it is capable of processing a common alert protocol.

The second requirement that we have for State and local officials is that they enter into a memorandum of agreement with FEMA to establish what is called a common operating group, or a COG. That group is similar to a distribution list that allows the State or local government to share information inside of the system.

The third step that if they wish to become a public alerting authority is that they have to enter into a memorandum of agreement that defines the geographic area that they are requesting this public alerting authority for, as well as the types of messages that they intend to send through the system and the dissemination channels over which that information would go.

The last step that is required of the State and local governments is that they take our IS–247.A course. That is the IPAWS training that is administered by the Emergency Management Institute. Since 2013, we know that there have been well over 20,000 people have taken that training.

In addition to that memorandum of the requirements of the MOA, we also require that every person that interfaces with that software, that touches IPAWS, also take that IPAWS IS–247.A training. We make additional resources available to State, local, Tribal, and territorial governments through our lab that is located in Indian Head, Maryland so that they can maintain proficiency in the use of the software.

That affords them the opportunity to create test messages in a safe environment and return the results to them so that they have a clear understanding of how that message will appear over radio, television, as well as wireless emergency alerts on mobile devices.

Mr. PAYNE. Are you planning additional requirements with respect to, you know, on-going training and that type of thing, you know, with this, you know, the human error that was cause for a false alarm in Hawaii? What is the redundancy that we can look for so we take that out of the equation as much as possible?

Mr. JOHNSON. Thank you, Congressman. One of the things that I will share is we were already undergoing a complete review of our training courses that are hosted by the Emergency Management Institute.

We will, likewise, double back and conduct additional reviews of that training to ensure that these type of scenarios or similar type of events that occurred in Hawaii on January 13, as well as others that we have observed across the country, are properly factored into our training offerings.

We will look into making additional training beyond our IS–251 course, which is a more advanced training that we encourage alerting authorities to take. We are looking at revamping that and considering refresher training on an annual basis as well.

Mr. PAYNE. OK.

Well, Mr. Chairman, my time is just about up, so I will yield so Ms. Jackson Lee can——

Mr. DONOVAN. The gentleman yields.

The Chair recognizes Ms. Jackson Lee from Texas.

Ms. JACKSON LEE. Let me thank the Chairman and the Ranking Member for their extended courtesies and thank the witnesses for their presence here today. Although we are asking questions in a very calm manner, this had to be a hair-raising, on-fire incident.

In fact, it could have generated enormous loss of life by people's own panic. I guess if it had continued long, most of us—I remember visibly seeing a panicked parent putting his child in a manhole. That will be a constant memory.

Certainly if it was a real incident, we know that people would be seeking any way to save their lives. One of the things that I wanted to take note of is if you all can comment, though you are here on the communications aspect, working with State emergency centers on how people do evacuate.

I did not get a sense from the video that people were even evacuating in any sort of orderly manner or even knew what to do, but I will—I will put that on the table as a concern.

But let me indicate that the individual employee has broken his silence and said that he didn't—it was real. He didn't hear any words 'exercise, exercise.' It was real, and he maintains that.

I would like you to respond to that, but I also want you to respond to these questions that, as I understand the facts, that once the mistake was realized, the employee who initiated the real-world alert was prompted to send out the cancel message on something called AlertSense, but at no point did the employee assist in the process. Has any of your agencies looked extensively as to why that did not happen?

Then, secondarily, since this is such a massive notice, and Hawaii is so positioned in the Pacific, and I understand there was a call to the Pacific Command, or that it is well-connected because he indicated that there was a missile alert, that there was no safeguard measures to withdraw the alert.

So if you would answer the questions about the employee's, or not respond to employee's, but that there was his representation that it was an incident without the "exercise, exercise", how that could be possible?

No. 2, how it could be possible, if you're prompted, was that discovered that you were prompted to send out a cancel message on AlertSense and that was not done? Or is that automatic so that the employee, or the person who was obviously in shock or whatever their condition was, that the alert goes out automatically? That it should be canceled?

Then, were there no safeguards, measures to withdraw the alert? If you could answer those, I would appreciate it.

Ms. FOWLKES. With respect to the employee's statement that there was no "exercise, exercise, exercise" at the front and end, we actually sent agents to Hawaii to speak to personnel and the Hawaii Emergency Management Agency.

From the information that they have given us, and as well as other discussions that we have had including other people that

were in the room, there was at the beginning and at the end, "exercise, exercise, exercise."

Now, the warning officer who transmitted the alert has refused to talk to the FCC, but in discussions with Hawaii Emergency Management, he submitted a written statement in which he claims he didn't hear the "exercise, exercise, exercise" at the beginning or the end.

Now, the problem with the alert wasn't the "exercise, exercise, exercise." The problem was with their respect to their script. It said, "This is not a drill", which wasn't consistent with Hawaii's Emergency Management Agency.

He claims, at least according to that statement, that that is all he heard, and so he thought it was a live event and, ergo, initiated a live alert.

With respect to cancellation and correction, just to explain, the cancellation piece only stops the alert from retransmitting. So for example on WEA, if you have your cell phone off, and they issue a cancellation, then your phone won't get it. So the cancellation, in and of itself, which they were able to do, didn't solve all of the problem.

The bigger problem was that from the preliminary findings that we have made is that Hawaii Emergency Management Agency never contemplated the possibility that they would ever issue a false alert and so they did not have protocols in place, standard operating procedures, to address that.

With respect to the WEA and EAS, they had to figure out what code to issue. They talked to FEMA personnel on what was about a 45-second phone call. Then somebody had to go log in and actually write the correction message because they did not have a template for that.

So that was really the problem with the delay in issuing the correction. They never contemplated that they would ever have a false alert. Do in this instance when it happened, they weren't prepared for it.

Ms. JACKSON LEE. You wish to comment?

Mr. JOHNSON. Thank you. Your question about an automatic withdrawal of the information from or the message from the system——

Ms. JACKSON LEE. Right, because they had to write, as she said, they were sending out emails and posting it on their personal Facebooks is one of the ways they were responding.

Mr. JOHNSON. Yes, so as Ms. Fowlkes described, with the cancellation of the message, which we know took place within minutes, as she described, that automatically takes the message out of the network so that it is not rebroadcast. That is a deliberate action that the employee had to take to cancel that message within the network.

The follow-up message to send out a corrective, kind-of a corrective action-type message, was also a deliberate action that the Hawaii Emergency Management, the agency, was not prepared for.

Typically, we exercise for success when it comes to the types of messages that we send and the deliberate actions that we would wish the public to take.

In this case, I would say that if there was any confusion on the part of Hawaii Emergency Management as to their authority to send that message, or if there was any question as to the type of message that should be sent, and in this case, it was a civil emergency message that was issued to correct the error that had occurred at 8:07.

When there is that type of uncertainty in the community, that points back, in my opinion, to some of our training offerings. That is where we are going to address this is through training and increased awareness and working with our Federal, State, and local partners.

But those are all deliberate actions on their part that they must take and be prepared for in terms of addressing any type of error that occurs with some errant message that is put out in the system.

Ms. JACKSON LEE. I am going to yield back.

I want to thank the Ranking Member—well, let me thank the witnesses, and let me thank the Ranking Member and the Chairman for their courtesies.

I just want to pose this question on the record, not for an answer. I am maybe getting pieces of this, but to me it appears that this should be raised to a Federal level, establishing protocols.

This was, I think, was one of the more frightening incidences that happens in a State, and the State is left to their own devices and protocols which they did not have. This could have been catastrophic.

So I yield back with that question posed. Thank you so very much.

Mr. DONOVAN. I want to thank the witnesses for your valuable testimony. Members of our subcommittee may have additional questions for the witnesses, and I would ask that you would respond to those in writing.

This panel is now dismissed. I ask the clerk to prepare the witness table for the second panel. Thank you both very much for sharing your expertise with us.

Mr. JOHNSON. Thank you.

[Recess.]

Mr. DONOVAN. I would like to welcome our second panel to today's hearing, and thank all of you for your participation.

Mr. Benjamin Krakauer serves as the assistant commissioner for Strategy and Program Development at the New York City Emergency Management Department. He currently serves on FEMA's National Advisory Council Integrated Public Alert and Warning Committees.

I would now like to yield to the gentleman from New Jersey, Mr. Payne, to introduce our next witness.

Mr. PAYNE. Thank you, Mr. Chairman.

I have the distinct pleasure of introducing Director Peter T. Gaynor, is the director of Rhode Island Emergency Management Agency and was appointed by Governor Gina Raimondo in January 2015.

As the director, he serves as the policy advisor to the Governor on emergency management matters and serves as the liaison be-

tween the Federal Emergency Management Agency and all local emergency management offices throughout the State. Welcome, sir.

Mr. DONOVAN. Mr. Scott Bergmann serves as senior vice president of Regulatory Affairs at Cellular Communications Industry Association and is responsible for coordinating Federal regulatory issues for the association affecting the wireless industry, including spectrum, broadband, and public safety policy making.

Mr. Sam Matheny——

Mr. MATHENY. Matheny——

Mr. DONOVAN. Matheny. I had it, Sam—is the chief technical officer at the National Association of Broadcasters. He is also a member of the FCC Communication's Security Reliability and Interoperable Council and a member of the Academy of Digital Television Pioneers.

The witnesses' full written statements will appear on the record. I thank you all for appearing today and sharing your expertise with us.

The Chair now recognizes Mr. Krakauer for 5 minutes.

STATEMENT OF BENJAMIN J. KRAKAUER, ASSISTANT COMMISSIONER, STRATEGY AND PROGRAM DEVELOPMENT, NEW YORK CITY EMERGENCY MANAGEMENT, CITY OF NEW YORK, NEW YORK

Mr. KRAKAUER. Thank you, Chairman Donovan, Ranking Member Payne, and Members of the subcommittee for the opportunity to speak with you today about emergency alerts and warning.

We take this issue very seriously in New York City and have invested considerable resources in it over the past decade, thanks in part to funding from the Urban Area Security Initiative.

New York City's opt-in emergency public information system, Notify NYC, began in 2007 and to date has sent out more than 10,000 messages. New York City Emergency Management maintains a cadre of public warning specialists who work in our 24/7 emergency operations center around the clock.

The majority of our messages are translated into the top 13 languages spoken in the city, including American sign language. Nearly 675,000 people have enrolled in Notify NYC, and we have begun to see large increases through our recently-released mobile application which allows users to get messages based on their present location, has a mapping interface so users can view their location relative to the location of an emergency, and streamlines the enrollment process to promote user adoption.

While we are very proud of Notify NYC and continue to market and promote it across New York City's 675,000 subscribers, in a city of 8.5 million residents it is not enough.

To expand our reach during the most critical emergencies, New York City relies on the Federal Wireless Emergency Alert System. New York City helped test the system with FEMA, the FCC, and the wireless industry in 2011 and has activated the system 8 times since 2012: Three times during Hurricane Sandy, 2 announcing travel bans in response to severe winter weather, and 3 related to the terrorist bombing in Chelsea.

Our experience with WEA during emergencies shows us the power of the system, but it also highlights its shortcomings. We ap-

preciate the attention that the FCC has paid to our concerns adopting rules that permit the inclusion of links and telephone numbers, improved geo-targeting requirements, and will soon allow longer messages and messaging in Spanish.

However, the new rules are not as comprehensive as we would hope and therefore we feel that the effectiveness of the system is still limited.

For example, missing from the FCC's latest order is multi-media alerting, many-to-one communication, and multi-lingual learning beyond Spanish. Further, the law still permits consumers to opt out of receiving WEA messages from localities, which we strongly oppose.

We must have the ability to embed multimedia in WEA messages. This major gap was demonstrated when the NYPD needed the public's assistance in locating the suspected Chelsea bomber before he detonated another device.

New York City issued a city-wide WEA that included the suspect's name, age, instructions to call 9–1–1 if seen, and a statement, "See media for pic." Since there is no capability to include images in WEAs, unlike the tens of millions of picture and video messages that are sent between consumers on a daily basis, recipients of the message needed to find a different source to see the suspects photo.

To quote a recent letter sent to Chairman Pai from New York City Police Commissioner James O'Neill, "We cannot continue to rely on the public taking this extra step. The law enforcement community can no longer afford to depend on a wireless emergency response system that is lagging far behind what technology can offer."

"The Chelsea bombings highlighted this major weakness in the wireless emergency alert system. Millions of New Yorkers who wanted to help us find the suspect were given no other option but to take the additional time to search for his photo. That time is often a commodity we can't afford to waste."

In surveying New Yorkers after the fact, we found that only 45 percent of message recipients took that extra step to look for the photograph.

Today's WEA system is one-directional and does not permit users like New York City to determine how many devices received a message, nor does it offer the public the ability to respond to a WEA to provide information back to us.

The ability to rapidly collect and aggregate de-identified but location-specific information would allow for the more efficient deployment of scarce resources following an emergency.

When the WEA system was first created by Congress, it required that the public have the right to opt-out of receiving messages from all originators except for the President.

A common tenet among emergency managers is that all emergencies begin and end locally. Local alert originators need the unfettered ability to reach messages during an emergency.

False alerts and poorly-targeted messages lead to consumer opt-outs and prevent people from receiving future messages that may save their life. We encourage Congress to change the law to eliminate the opt-out provision.

In closing, the Wireless Emergency Alert System is one of the greatest advances in public alerting warning in our country's history and has been used thousands of times across the country to protect lives and property.

It is a cornerstone element of our public alert and warning strategy in New York City, however, the capability offered by WEA has not kept up with the advances in technology and with how people use their mobile phones.

WEA needs further enhancement to support today's threats and hazards. New York City looks forward to working with Congress, our Federal partners, and the wireless industry to improve this important tool. Thank you.

[The prepared statement of Mr. Krakauer follows:]

PREPARED STATEMENT OF BENJAMIN J. KRAKAUER

FEBRUARY 6, 2018

INTRODUCTION AND HISTORY OF PUBLIC ALERTING IN NEW YORK CITY

Thank you, Chairman Donovan, Ranking Member Payne, and Members of the subcommittee for the opportunity to speak with you today about the very important topic of emergency alerts and warnings. This is a topic that we take very seriously in New York City and have invested considerable resources in over the past decade, thanks, in part, to funding from the Urban Area Security Initiative. New York City's emergency public information system, called Notify NYC, began as a pilot program in 2007 following the tragic Deutsche Bank fire on Liberty Street in Manhattan. This fire blanketed Lower Manhattan with smoke and ash but the city did not have the ability to proactively issue a warning. In 2009, Notify NYC began offering services city-wide as an opt-in service. Since the inception of the program, New York City Emergency Management has considered public alert and warning to be a full-time job and our agency maintains a cadre of Public Warning Specialists who work in Watch Command, a 24×7 operations center responsible for coordinating emergency activity in New York City on a daily basis. There is always a Public Warning Specialist on-duty and his or her primary function is to issue public alerts and warnings as quickly and accurately as possible.

Since the program's inception, we have issued more than 10,000 messages. With more than 200 languages spoken in New York City, most of our messages are translated into the top 13 languages, including American Sign Language through a linked website. By mid-2019, we'll offer multilingual messaging to our subscribers directly through e-mail, text message, and telephone call. Enrollment in the program increases every year and today, almost 675,000 people have enrolled to receive Notify NYC messages via e-mail, telephone call, text message, and through social media. Most recently—during National Preparedness Month in September 2017—we released a mobile application dedicated to public alert and warning in New York City. This state-of-the-art application is location-aware, allowing users to get messages based on their present location and not just pre-registered locations, has a mapping interface so users are able to view their location relative to the location of an emergency, and streamlines the enrollment process to promote user adoption.

WIRELESS EMERGENCY ALERTS IN NEW YORK CITY

While we are very proud of the emergency public information system that we've built and work tirelessly on marketing and improving the program, we recognize that 675,000 subscribers in a city of 8.5 million residents is not enough. Additionally, we know that there are large populations that we need to reach during emergencies that are unlikely to enroll in the city's notification system, including more than 60 million annual tourists and business travelers who are only in the city for a short period of time. To reach these individuals New York City relies on the Federal Wireless Emergency Alert—better known as WEA—system to deliver high-priority, time-sensitive messages to mobile phones. The beauty of WEA is that it is an opt-out system, and the messages that consumers receive are based on their present location, not their home or billing address.

New York City has a strong history with WEA. The program was originally announced at the site of the World Trade Center and New York City Emergency Management worked with the Federal Emergency Management Agency, the Federal

Communications Commission, and the wireless industry on testing the WEA system in 2011. In 2012, New York City became the first State or local government in the country to issue a WEA message announcing the evacuation order ahead of Hurricane Sandy. Since gaining access to the WEA technology New York City has activated the system 8 times: Three messages related to Hurricane Sandy, 2 messages announcing travel bans related to severe winter weather, and 3 messages in response to the terrorist bombing in Chelsea.

THE NEED FOR WEA ENHANCEMENTS

Our experience with WEA messages during actual emergencies underscores the power of the system but also highlights many of its shortcomings that we feel need to be addressed in the near term. Before I discuss our top issues, let me say that New York City appreciates the attention that the FCC has paid to this important issue. Since the FCC released its first Notice of Proposed Rulemaking in 2015, rules have been adopted that permit the inclusion of links and telephone numbers in WEA messages, require geotargeting below the county level, and—as of May 2019—will allow for messaging in Spanish and expand the number of available characters from 90 to 360 which will make it easier for emergency managers to provide detailed, actionable information. On January 30 of this year, the FCC also adopted a number of rules that have had broad support by emergency management and public safety agencies across the country including requiring WEA messages to be preserved on the device for 24 hours and, most importantly, improved message geo-targeting.

While these are enhancements are long overdue and welcomed, the new rules do not go far enough and continue to limit the effectiveness of the WEA system. Missing from the FCC's latest order is multimedia alerting, "many-to-one" communication, and multilingual alerting beyond Spanish; Further, the law still permits consumers to opt out of receiving WEA messages, except those issued by the President of the United States.

MULTIMEDIA ALERTING

There is currently no ability to embed multimedia—like images, maps, infographics—in WEA messages. This major capability gap was exemplified on Monday, September 19, 2016 when NYPD needed the public's assistance in locating the suspected bomber before he placed or detonated another device. Within minutes of receiving the request our office issued a city-wide WE! that included the suspect's name, age, instructions to call 9–1–1 if seen, and a statement "see media for pic;" Instead of being able to include an image in the message—like the tens of millions of picture and video messages that are sent between consumers on a daily basis—recipients of the WEA message needed to take an extra step and go to a different source in order to see an image of the suspect. To quote a recent letter sent to Chairman Pai from New York City Police Commissioner James O'Neil:

"We cannot continue to rely on the public taking this extra step, and when it comes to our city's most critical cases, the law enforcement community can no longer afford to depend on an emergency wireless response system that is lagging far behind what technology can offer . . . Pictures provide instant recognition and speak a universal language . . . the Chelsea bombings highlighted this major weakness in the Wireless Emergency Alert system: millions of New Yorkers who wanted to help us find the suspect were given no other option but to take the additional time to search for his photo. In any case like this, that time is often a commodity we can't afford to waste."

Following this instance, New York City commissioned a survey of New Yorkers who received the WEA to determine what action, if any, they took upon receiving the WEA message. While 89 percent of New Yorkers felt that our use of WEA in this case was appropriate, only 45 percent of message recipients took the extra step to look for the photo.

MANY-TO-ONE

Today's WEA system is one-directional and does not offer emergency management and public safety the ability to determine how many devices received a message nor does it offer the public the ability to respond to the WEA message to provide information back to Government. In 2010, a severe thunderstorm with embedded tornadoes caused damage to buildings, vehicles, infrastructure, and more than 7,000 trees in New York City. In order to identify the hardest-hit areas, city residents were asked to report damage by calling 3–1–1. The information provided was then sorted, mapped, and analyzed in order to determine the hardest-hit areas, a process that

took hours but could take minutes by leveraging the broad reach of WEA messages and adding the ability for the public to reply to messages. Simply put, the ability to rapidly collect and aggregate de-identified but location-specific information would allow for the more efficient deployment of scarce resources following an emergency.

OPTING OUT & NATIONAL THREATS

When the Wireless Emergency Alert system was first created by Congress, it required that the public have the right to opt out of receiving messages, except those issued by the President of the United States; While New York City respects consumer choice and supports the President's need to alert the country during National emergencies, it is important to note that all emergencies begin and end locally and local governments need the same unimpeded ability to reach their populations. False alerts, like the unfortunate situation in Hawaii, and poorly-targeted messages likely lead to consumer opt-outs and will prevent those from receiving future messages that may save their life. As such, we encourage Congress to change the law to eliminate the opt-out provision. Such a change, combined with other WEA improvements, will help to ensure that critical warnings reach their intended audience. With respect to National threats, like an in-bound missile, New York City feels that the Federal Government, as part of its National defense responsibility, is in the best position to issue timely warnings. We encourage Congress to work with the Departments of Defense and Homeland Security on operationalizing the ability for issuance of public alerts when an in-bound missile—or similar—threat is detected.

CONCLUSION

In closing, the Wireless Emergency Alert system is one of the greatest advances in public alert and warning in our country's history and has been used thousands of times across the country to protect lives and property and is a cornerstone element of our public alert and warning strategy in New York City. However, the capability offered by WEA has not kept up with the times and needs further enhancement in order to support the response to today's threats and hazards; New York City looks forward to working with Congress and our Federal partners on continuing to improve this important tool. Thank you.

Mr. DONOVAN. Thank you, Mr. Krakauer.

The Chair now recognizes Mr. Gaynor for 5 minutes.

STATEMENT OF PETER T. GAYNOR, DIRECTOR, RHODE ISLAND EMERGENCY MANAGEMENT AGENCY, STATE OF RHODE ISLAND

Mr. GAYNOR. Good morning, Chairman Donovan, Ranking Member Payne, distinguished Members of the subcommittee. It is a pleasure to appear before you today to discuss the critical importance of reliable alert notification communication systems at the State, local, and Federal levels that we depend on within the State of Rhode Island to successfully achieve our mission.

These systems, plans, policies shape that shape their use and the personnel that train, maintain, and operate them are a core function of preparedness and response across the country.

My name is Pete Gaynor, and I am the director for Emergency Management for the State of Rhode Island. I am also the chair for the State's Interoperable Communications Committee responsible for ensuring alert notification and communications systems are properly governed, aligned, and integrated. I have submitted my full statement to the committee, which I ask be made part of this hearing today.

Today I want to briefly describe to the subcommittee first a snapshot of those alert and warning communications systems and their use within the State of Rhode Island; second, what we have done since the Hawaii false alert; and finally, some insights and rec-

ommendation for a stronger, more resilient alert and warning communications system Nation-wide.

First, let me describe our system from the local level up. In 2015, the State of Rhode Island invested in a commercial mass notification system called Code Red.

Using the Emergency Management Performance Grant, we purchased on behalf of all the communities, 39 communities and selected State agencies, a singular common system in order to remove duplication of effort, improve operational efficiencies and save precious local, State, and Federal funding resources.

Authorized and trained agents at the local level can launch any public safety-related alert within their jurisdiction. The State has the capability to launch on the behalf of any single municipality, multiple municipalities or the entire State, depending on the threat or hazard.

In 2017, August 2017, we completed a long overdue update of the State's emergency alert system plan and system. We have spent significant energy to ensure plans, procedures, equipment, training, safeguards, and testing are up-to-date and fully operational. This remains an on-going priority for the State.

We continue to rely on other core Federal systems, such as FEMA's National warning system and National radio system to ensure we have multiple communication paths.

Since the January 2018 Hawaiian false ballistic missile alert was issued, we have redoubled our efforts through new plans, procedures, policies, redundancies, training, authorized users, the functionality of equipment, interoperability, and the safety measures to ensure we fully understand the strengths, the weaknesses, and the potential gaps of all our alert warning and communication systems.

We have revalidated our internal launch and approval process to ensure prescriptive messaging is common across all our platforms to include recall messaging should an erroneous alert be triggered. This process continues today.

In New England, at both the State and Federal level, we are in the process of reviewing past practice for alert and warning procedures such as those outlined in FEMA's National Warning System operations manual, to make sure that the published guidelines and instructions are logical, executable, and reasonable after what happened in Hawaii.

As outlined in the manual, threats posed by National and manmade disasters or enemy attack make it imperative for State, local, territorial, and Tribal governments to have access to an effective and reliable means of communication with which to warn the public of impending emergencies so they make take preventative actions.

My fellow New England directors and I completely support the premise and are working diligently to ensure we have a safe, secure, and reliable alert and warning system.

In conclusion, in addition to reviewing and validating our systems, I believe we have created what I call a technology trap. I believe this problem is similar to the military with their GPS and digital mapping.

Will our soldiers be able to navigate with a pencil and a paper map and a compass should the GPS constellation be disrupted? Can we as emergency managers communicate in a world where any combination of a cyber attack, power disruption, or natural hazard takes out our digital alert and warning communication networks?

Are we ready to communicate in and warn in an analog world? Can we communicate to our citizens without cellphones and the internet communicating in a degraded environment?

Finally, review the DHS security clearance program to ensure the right decision makers to route every level of the emergency management system have the correct clearance level so matters like threat briefs and critical time secure communications can seamlessly, rapidly, and securely occur.

Thank you, Chairman Donovan and subcommittee Members for the opportunity to appear in front of you today.

[The prepared statement of Mr. Gaynor follows:]

PREPARED STATEMENT OF PETER T. GAYNOR

FEBRUARY 6, 2018

Good morning Chairman Donovan, Ranking Member Payne, and distinguished Members of the subcommittee. It is a pleasure to appear before you today to discuss the critical importance of reliable alert, notification, and communication systems at the local, State, and Federal levels that we depend on within the State of Rhode Island to successfully achieve our mission. These systems, the plans and policies that shape their use, and the personnel that train, maintain, and operate them, are a core function of preparedness and response across the country.

My name is Pete Gaynor and I am the director of Emergency Management in the State of Rhode Island. I am also chair of the State's Interoperable Communication Committee (ICC) responsible for ensuring alert, notification, and communication systems are properly governed, aligned, and integrated. As the director and a professional emergency manager, I am responsible for preparing for emergencies, coordinating the activation and use of resources, ensuring an integrated and unified response, and managing the recovery effort in support of our local and State governments, citizens, and businesses.

I am pleased to be testifying before the subcommittee today. I have submitted my full statement to the committee, which I ask to be made part of the hearing record.

Today, I want to briefly provide the subcommittee with, first a snapshot of those alert, warning, and communications systems and their use within the State of Rhode Island, second, what we have done since the Hawaii false alert; and finally, some insights and recommendations for a stronger more resilient alert, warning, and communications system Nation-wide.

Let me describe our system from the local level up. In 2015, the State of Rhode Island invested in a commercial mass notification system called CodeRED. Using the Emergency Management Performance Grant, we purchased on behalf of all 39 municipalities and selected State agencies, a singular common system in order to remove duplication of effort, improve operational efficiencies and to save precious local, State, and Federal funding resources. Authorized and trained agents at the local level can launch any public safety-related alert within their jurisdiction. The State has the capability to launch on behalf of a single municipality, multiple municipalities, or the entire State depending on the threat or hazard.

With the implementation of the Integrated Public Alert and Warning Systems—IPAWS, we have been able to seamlessly integrate CodeRED in order to complement the Federal Emergency Alert System (EAS) and Commercial Mobile Alert System (CMAS).

In August 2017, we completed a long-overdue update of the State's EAS Plan. We have spent significant energy to ensure plans, procedures, equipment, training, safeguards, and testing are up-to-date and fully operational. This remains an on-going process.

Since 9/11, Rhode Island has been fortunate to receive Federal funding to build and maintain what we believe is a first-class, border-to-border, interoperable Land Mobile Radio (LMR) system called the Rhode Island State-wide Communications Network, or RISCON. RISCON allows thousands of our first responders to

seamlessly operate in any corner of the State, to include cross-border to many of our Massachusetts and Connecticut communities.

To ensure redundancy and interoperability throughout the State, we have a VHF system called the Emergency Management State Radio System (EMSTARS) which connect all local emergency managers. That system is being refreshed this year. We also have the Rhode Island Law Enforcement Telecommunication System (RILETS) which is a data system mainly dedicated for daily coordination of local and State police departments.

We continue to rely on other core Federal systems such as FEMA's National Warning System (NAWAS) and the FEMA National Radio System (FNARS) to ensure we have multiple communication paths, such as non-switched terrestrial voice circuits and High Frequency (HF) radio for both voice and data.

Since the January 13, 2018, Hawaiian false ballistic missile alert was issued, we have redoubled our efforts to review plans, procedures, policies, redundancies, training, authorized users, functionality of equipment, interoperability and safety measures to ensure we fully understand the strengths, weaknesses, and potential gaps of all of our alert, warning, and communication systems. We have re-validated our internal launch and approval process, ensured pre-scripted messaging is common across all of our platforms, to include recall messaging should an erroneous alert be triggered. This review process continues today.

In New England, at both the State and Federal level, we are in the process of reviewing past practices for alert and notification procedures, such as those outlined in the July 2016 FEMA Manual 211–2–1, NAWAS Operations to make sure published guidelines and instructions are logical, executable, and reasonable after what occurred in Hawaii.

As outlined in the manual, "threats posed by natural and man-made disasters or enemy attack make it imperative for State, local, territorial, and Tribal governments to have access to an effective and reliable means of communication with which to warn the public of impending emergencies so that they may take protective actions." My fellow New England directors and I completely support this premise and are working diligently to ensure we all have a safe, secure, and reliable alert and warning system.

We also rely on a host of social media platforms like Twitter and Instagram to share and collect information. We also look forward to the deployment and use of FirstNet, however in the light of recent events and the growing complexity and interdependency of many of these technologies, we must proceed with caution and apply applicable lesson-learned to avoid past missteps.

In conclusion, in addition to reviewing and validating our current systems, I believe we have created what I call the Technology Trap. I believe our problem is similar to the challenge the military has with GPS and the digital mapping world—will our soldiers still be able to navigate with a pencil, paper map, and magnetic compass should our GPS constellation be disrupted? Can we as emergency managers communicate in a world where any combination of a cyber attack, power disruption, and/or natural hazard takes out our digital alert, warning, and communications networks? Are we ready to communicate, alert, and warn, in an analog world? Can we communicate to our citizens without cell phones and the internet? The harsh reality is if you can't communicate, you can't govern.

Some recommendations:

- Ensure FEMA alert and warning procedures are aligned to present-day threats and shifts in technology to include clearly defining responsibilities between all levels of government for alerts and warnings.
- Develop a National concept of operations on how to better use General Mobile Radio Service (GMRS), Family Radio Service (FRS), Travelers' Information Station (TIS or Highway Advisory Radio), service with a focus on how to network these systems with State and Federal systems in order to enhance our ability to communicate with the public in an austere environment.
- Encourage additional training and exercises at every level to ensure leaders and operators are familiar with every detail of every communication, alert and warning systems, procedures, and shortfalls. I would encourage a more robust and regular Nation-wide IPAWS testing program focusing on the fundamentals of communicating in a degraded environment.
- Review the DHS Security Clearance program to ensure the right decision makers, throughout every level of the emergency management system have the correct clearance level, so matters like threat briefs and time-critical secure communications can seamlessly, rapidly, and securely occur.

Thank you, Chairman Donovan and subcommittee Members, for the opportunity to appear before you today.

I stand ready to answer any questions you might have.

Mr. DONOVAN. Thank you, Mr. Gaynor.

The votes are called. We are going to try to get through your testimony first then take a short break, and we will come back for questions.

The Chair now recognizes Mr. Bergmann.

STATEMENT OF SCOTT BERGMANN, SENIOR VICE PRESIDENT, REGULATORY AFFAIRS, CTIA

Mr. BERGMANN. Chairman Donovan, Ranking Member Payne, and Members of the committee, thank you for the opportunity to testify today about the critical and successful role of wireless emergency alerts.

CTI and the wireless industry commend Congress for passing the Warning Act, which established the wireless emergency alert or WEA, a partnership between the wireless industry, Government, and public safety officials.

Since its launch 5 years ago, wireless emergency alerts have become an essential tool for Americans, hundreds of millions of Americans, who rely on their mobile phones every day. Today, wireless providers who serve over 99 percent of U.S. subscribers participate in WEA voluntarily.

More than 33,000 wireless emergency alerts have been sent helping to locate those in danger and warn of imminent threats or disasters. CTI members are deeply committed to ensuring that WEA remains a trusted, secure, and effective resource for the American public.

So the recent false alarm in Hawaii underscores the importance of our collective efforts to ensure the functionality and the integrity of our Nation's emergency alert systems.

With that in mind, my testimony today will address the vital role that WEA plays, our on-going efforts to improve its capabilities, and the importance of maintaining the system's integrity.

A decade ago, Congress recognized the value of wireless emergency alerts to reach Americans wherever they are. Now, as more than half of American households are wireless only, WEA has become an essential tool for public safety.

As part of our broader National alerting system, Federal, State, and local authorities transmit emergency messages to FEMA, FEMA authenticates and formats those messages and sends them out to the various different alerting systems.

Wireless providers deliver authorized WEA messages to a particular geographic area as determined by the alert authorities. Wireless providers do not control the content of messages and do not exercise discretion over whether to send them.

Because local authorities can target specific geographic areas, they are extremely effective at reaching those Americans directly impacted by an emergency. WEA's unique sound and vibration help ensure that everyone can be aware of the alert.

Wireless emergency alerts have helped to address terrorist threats, locate suspects like in the 2013 Boston bombing and the 2016 Chelsea bombing, and they have helped to return abducted children and they have warned millions of people in the path of severe weather events.

We continue to expand and improve WEA's capabilities. In the past year, the FCC adopted rules to expand the content that authorities can send, adding additional characters, Spanish language, blue alerts and downloadable content through embedded links, as well as supporting additional testing by State and local authorities.

The wireless industry has supported these enhancements because our Members are committed to the proven life-saving success of WEA. Just last week, the FCC adopted an order that further improves WEA's geotargeting capability.

Today, WEA alerts can be targeted down to the cell-sector level, a significant improvement over the original county-level targeting. The FCC's new approach will take advantage of innovative device-based solutions to further target those alerts.

The wireless industry is undertaking significant standards, testing, and deployment work to support this capability. The FCC's deadlines are aggressive, but the wireless industry will work intently to implement them.

Finally, the false alert in Hawaii underscores that public confidence must be our highest priority. Alert originators must send warnings appropriately and judicially. FEMA must authenticate messages quickly and accurately and providers must deliver them to the targeted area.

We commend this committee and Chairman Pai at the FCC for working quickly to identify lessons learned from the false alert. We appreciate Commissioner Rosenworcel's call for additional best practices.

While there will be many lessons learned, this event does demonstrate that the technical capabilities of WEA function. Policy makers and the public should have confidence that in the event of a real emergency, wireless emergency alerts can send information rapidly and effectively.

Let me also stress that the wireless industry is keenly focused on the security of our networks, including those that support WEA. Through a combination of technologies, policies, and best practices, we work closely with our Government and public safety partners to further our common goal of a trusted WEA system.

CTI is proud of the critical role that we have played in our National system, and we are committed to working collaboratively to maintain public confidence.

Thanks for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Bergmann follows:]

PREPARED STATEMENT OF SCOTT BERGMANN

FEBRUARY 6, 2018

Chairman Donovan, Ranking Member Payne, and Members of the committee, on behalf of CTIA and our member companies throughout the wireless ecosystem, thank you for the opportunity to appear before you today to discuss the critical and successful role of Wireless Emergency Alerts within our Nation's emergency alert system.

CTIA commends the bi-partisan leadership in Congress for its passage of the Warning, Alert, and Response Network (WARN) Act, which created the Wireless Emergency Alert (WEA) program, a public-private partnership between the wireless industry, Government, and alert originators. The Wireless Emergency Alert system was launched in 2012 and is jointly implemented and administered by the Federal Communications Commission (FCC) and Federal Emergency Management Agency

(FEMA). In the 5 years since the launch of the Wireless Emergency Alert system, it has become a critical resource for the hundreds of millions of Americans who rely on their mobile phones every day.

CTIA and its member companies are proud of the wireless industry's role in the Wireless Emergency Alert system. Today, all four National wireless providers and dozens of regional providers, serving more than 99 percent of all U.S. subscribers, are voluntarily participating in the Wireless Emergency Alert system; transmitting thousands of alerts each year and helping our public safety professionals save lives.[1] Ensuring that Wireless Emergency Alerts remain a trusted source of emergency information for the American public is one of our highest priorities.

The false alert that was issued in Hawaii on January 13, 2018 is of course at top of mind for policy makers, CTIA and its member companies, all WEA stakeholders, and the public writ large. The Hawaii incident underscores to all of us the importance of the functionality and integrity—and credibility—of our Nation's emergency alert systems. Any incident that affects the public's confidence in emergency alerts risks undermining the effectiveness of all alerting systems, including WEA. We lose the effectiveness of emergency alerting if people simply ignore or opt-out of receiving these critical messages.

For this reason, we are deeply committed to doing our part to ensure that Wireless Emergency Alerts remain a trusted and effective tool for public safety within our Nation's emergency alert system, which is managed by FEMA through the Integrated Public Alert and Warning System (IPAWS) that also supports the Emergency Alert System (EAS), National Weather Service, and other alerting tools. With that in mind, I would like to address the WEA program's success, the cooperative voluntary framework on which WEA operates, on-going efforts to enhance the geographic targeting (geo-targeting) of alert messages, and, finally, the importance of maintaining the WEA system's integrity.

THE SUCCESS OF WIRELESS EMERGENCY ALERTS

The Wireless Emergency Alert system is the newest and most effective means the Nation has for warning Americans of imminent dangers and other incidents requiring immediate action. A decade ago, Congress and this committee wisely recognized the value of wireless in reaching nearly every American and set in motion the creation of the Wireless Emergency Alert system. Now, as more than half of American households have cut the cord and are "wireless only,"[2] alerts and warnings sent to our mobile devices are the obvious choice for public safety officials to make sure we can take action wherever we are, whatever we are doing.

Wireless Emergency Alerts delivered to wireless devices in a targeted area—with their unique sounds, high volumes, and forceful vibrations—save lives. The WEA system sends out Amber Alerts and shelter-in-place directives, warns citizens of fires, floods, and tornados, and otherwise keeps the public apprised of real threats. Because WEA messages are delivered to consumers with capable mobile devices in an area targeted by local authorities, they are an extremely effective mechanism for reaching those Americans that are directly impacted by an emergency. It is no wonder that some have called Wireless Emergency Alerts "the Government's most potent public notification system."[3]

Since 2012, more than 33,000 Wireless Emergency Alerts have been sent to consumers with WEA-capable devices.[4] These messages have warned Americans of im-

---

[1] *Wireless Emergency Alerts,* Order on Reconsideration, 32 FCC Rcd 9621, 9625 n.28 (2017); see also, *CTIA, How Wireless Emergency Alerts Help Save Lives, https://www.ctia.org/consumer-tips/how-wireless-emergency-alerts-help-save-lives* (last visited Jan. 23, 2018).

[2] Stephen J. Blumberg & Julian V. Luke, Ctrs. for Disease Control & Prevention, Nat'l Ctr. for Health Statistics, *Wireless Substitution: Early Release of Estimates From the National Health Interview Survey, July–December 2016* (May 2017); see also, Alina Sleuth, Nat'l Pub. Radio, *The Daredevils Without Landlines—And Why Health Experts Are Tracking Them* (May 4, 2017), *https://www.npr.org/sections/alltechconsidered/2015/12/03/458225197/the-daredevils-without-landlines-and-why-health-experts-are-tracking-them.*

[3] Aaron C. Davis & Sandhya Somashekhar, *The only California county that sent a warning to residents' cellphones has no reported fatalities, Wash. Post*, Oct. 13 2017, *https://www.washingtonpost.com/investigations/the-only-california-county-that-sent-a-warning-to-residents-cellphones-has-no-reported-fatalities/2017/10/13/b28b5af4-b01f-11e7-a908a3470754bbb9__story.html?utm__term=.cd24bb9ecf9chttps://www.washingtonpost.com/investigations/the-only-california-county-that-sent-a-warning-to-residents-cellphones-has-no-reported-fatalities/2017/10/- 13/b28b5af4-b01f-11e7-a908-a3470754bbb9- __story.html?utm__term=.cd24bb9ecf9c.*

[4] Mark Lucero, Fed. Emergency Mgmt. Agency, *Integrated Public Alert & Warning System*16 16 (Aug. 8, 2017), *https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.napsgfoundation.org%2Fwp-content%2Fuploads%2F2017%2F08%2FFEMA__IPAWS-*

Continued

minent threats or disasters and asked the public for help in locating someone in danger.

For example, local emergency officials have used Wireless Emergency Alerts to inform the public of on-going law enforcement and terrorist threats, and to enlist their assistance. In 2013, Massachusetts authorities sent a shelter-in-place Wireless Emergency Alert while apprehending the suspects in the Boston Marathon Bombing.[5] And in 2016, the city of New York sent a description of the suspect in the Chelsea Bombing through a Wireless Emergency Alert, leading to the suspect's arrest within hours of the alert.[6]

In 2015, an AMBER Alert for a missing child was sent through the WEA system to wireless consumers in Minnesota. A citizen in the area received the alert on their smartphone, saw a black Honda Civic that matched the description issued in the alert, and called 9–1–1. Authorities responded and rescued the child from the abductor. This is just one of many such success stories of our National emergency alert system, which includes WEA—a total of 910 children have been successfully recovered through the AMBER Alert system, as of January 8, 2018.[7]

Wireless Emergency Alerts have also been used extensively to warn the public of severe weather emergencies. This past fall, more than 300 Wireless Emergency Alerts warned people around Houston, Texas about Hurricane Harvey and its rising floodwaters, more than 200 Wireless Emergency Alerts warned Floridians about the strong winds of Hurricane Irma, and Wireless Emergency Alerts played a critical role in warning many Californians about the devastating wildfires.[8] In 2013, 29 children were saved from a tornado ripping through a soccer building in Windsor, Connecticut when the camp manager received a Wireless Emergency Alert seconds before the tornado touched down.[9] Even as the system was only months old in 2012, public safety officials were using Wireless Emergency Alerts to warn the people in the path of Superstorm Sandy.[10]

For more than a decade, the wireless industry has worked diligently to develop and deploy this capability in its networks and devices. Through cell broadcast technology unique to the WEA system, mobile providers can broadcast Wireless Emergency Alerts from cell-sites in areas targeted by local emergency officials to wireless devices in a timely manner. Today, there are millions of devices throughout the United States that are capable of receiving these critical messages.

Wireless Emergency Alerts are part of the broader National alerting system, known as the Integrated Public Alert and Warning System (IPAWS), managed by FEMA. Through IPAWS, authorized Federal, State, and local authorities, known as alert originators, transmit emergency messages to a FEMA-operated system. FEMA's system authenticates and formats the message for distribution across a variety of channels, including the WEA system. Of note, the substance and distribution channel of an alert is determined by the Federal, State, or local government that originates the alert. Wireless providers deliver authorized WEA messages to the target area identified by the alert originator without input into the content of a message or discretion over whether or not to transmit it.

Reflecting the evolution of our mobile wireless networks and devices, the capabilities of the Wireless Emergency Alert system continue to advance in a remarkably short time frame. In less than 6 years since the voluntary Wireless Emergency Alert

---

__Keynote__MarkLucero__20170708.pptxhttps://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.napsgfoundation.org%2Fwp-content%2Fuploads%2F2017%2F08-%2FFEMA__IPAWS__Keynote__Mark-Lucero__20170708.pptx.

[5] Rick Wimberly, *Powerful Wireless Emergency Alerts Success Stories at Congressional Hearing*, Emergency Management, Oct. 24, 2013, *http://www.govtech.com/em/emergency-blogs/alerts/Powerful-Wireless-Emergency-Alerts-Success-Stories-at-Congressional-Hearing.html.*

[6] David Goodman & David Gelles, *Cellphone Alerts Used in New York to Search for Bombing Suspect, N.Y. Times*, Sept. 19, 2016, *https://www.nytimes.com/2016/09/20/nyregion/cellphone-alerts-used-in-search-of-manhattan-bombing-suspect.html.*

[7] *Amber Alerts*, Nat'l Ctr. for Missing & Exploited Children, *http://www.missingkids.com/gethelpnow/amber* (last visited Jan. 23, 2018).

[8] See generally CTIA, *Hurricane Harvey: Resiliency & Relief*, *https://www.ctia.org/hurricane-harvey/* (last visited Jan. 16, 2018); Davis & Somashekhar, supra note 3; Richard Perez-Pena, Fire Alert Sent to Millions of Cellphones Was California's Largest Warning Yet, N.Y. Times, Dec. 7, 2017, *https://www.nytimes.com/2017/12/07/us/cellphone-alerts-california-fires.html.*

[9] Wimberly, supra note 5; see also, David Owens & Chloe Miller, *National Weather Service Confirms Two Tornadoes Monday*, Hartford Courant, July 2, 2013, *http://articles.courant.com/2013-07-02/news/hc-tornado-warning-0702-20130701__1__windsor-locks-dome-national-weather-service-confirms.*

[10] Rick Wimberly, *CMAS/WEA Used Extensively for Hurricane Sandy*, Emergency Management, Oct. 31, 2012, *http://www.govtech.com/em/emergency-blogs/alerts/CMASWEA-Used-Extensively for-103112.html* (noting that "alerts were issued all along the eastern seaboard in Virginia, West Virginia, Maryland, New York, Massachusetts, New Hampshire, and Maine").

system was first launched, the FCC has adopted various updates and improvements, including an order to enhance WEA's geo-targeting capabilities that was adopted last week. In 2016, the FCC put rules in place to increase the maximum alert length from 90 characters to 360 characters for LTE wireless systems and future networks, as well as support additional local and State testing capabilities, Blue Alerts, Spanish-language alerts, and embedded links and phone numbers. In particular, the FCC noted that allowing embedded references to be included in WEA alerts "will dramatically improve WEA's effectiveness" and that commenters identified this capability as "the most critical among all of our proposed improvements to WEA."[11]

CTIA's member companies are working hard to add these new capabilities into the WEA system, and have already answered public safety's call to ensure that alerts are capable of including embedded links so that consumers will be able to go to a website to see a photo of the missing child or a suspected terrorist.

ENHANCED GEO-TARGETING REQUIREMENTS

Last week, the FCC adopted another order focused on the geo-targeting capabilities of the WEA system.[12] The FCC initially mandated targeting at the county level, but many participating providers began voluntarily supporting geo-targeting of Wireless Emergency Alerts well below the county level to enable local officials to minimize over-alerting. An appropriately-targeted WEA message can mitigate the possibility that an alert will cause distress or panic in areas not actually at risk and enhance public confidence in the emergency alert system. Today, participating providers deliver Wireless Emergency Alerts to a targeted area that best approximates the area identified by the alert originators down to the cell-sector level.

While the ability to geo-target Wireless Emergency Alerts down to the cell-sector level will remain a constant feature of the system, we share the expressed goal of public safety leaders to harness innovative location technologies to further minimize the possibility of over-alerting. For this reason, CTIA supports the framework for enhancing the geo-targeting capabilities of the WEA system that the FCC adopted last week. To deliver this new capability, wireless providers will shift from a solely network-based approach to target the alert area to one that also harnesses location capabilities within mobile devices. Once available, this capability will give local alert originators an additional tool to minimize the possibility that someone will receive an irrelevant Wireless Emergency Alert.

The FCC's geo-targeting Order proposes an aggressive implementation time line that will present a significant challenge for wireless providers and device manufacturers. As the Order notes, significant standards, deployment, and testing work remains to support this enhanced geo-targeting capability throughout the chain of the alert—from alert originators to FEMA's gateway to wireless networks to mobile devices. The wireless industry—including participating providers and device manufacturers—will work intently, as it always has, in an effort to meet the FCC's aggressive deadline.

MAINTAINING PUBLIC CONFIDENCE AND SYSTEM INTEGRITY AFTER HAWAII

The January 13, 2018 incident in Hawaii has underscored for all of us—Government and industry alike—that the success of Wireless Emergency Alerts relies on the public's trust. Trust in the system hinges on execution. Alert originators must send Wireless Emergency Alerts appropriately and judiciously; the FEMA authentication and verification process must be expeditious and robust; and participating wireless providers must deliver WEA messages to the targeted area. Only this way will the public know that when a Wireless Emergency Alert is sent, the danger is real.

This committee should be commended for focusing on what errors led to the false Hawaii alert and on drawing out lessons learned, particularly around the issue of system integrity and security. Going forward, we should strive to make sure that another harm does not take root—namely, the danger that the next time an alert is issued, that some will not take it seriously or refuse to evacuate. For this reason, CTIA and the wireless industry commend FCC Chairman Pai for swift action to investigate the cause of this incident and appreciate FCC Commissioner Jessica Rosenworcel's recent recommendations and suggestions for new best practices around the training and use of our Nation's emergency alert system.

---

[11] *Wireless Emergency Alerts*, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 11112, 11137–38 (2016).

[12] *Wireless Emergency Alerts*, Second Report and Order and Second Order on Reconsideration (rel. Jan. 31, 2018), available at *https://www.fcc.gov/document/fcc-improves-wireless-emergency-alerts-0*.

Notably, Congress recognized the need to train and equip our alert originators to more effectively use our Nation's emergency alert system when the IPAWS Modernization Act became law in 2015. And in 2016, the FCC encouraged emergency management agencies to engage in proficiency training exercises that could help minimize system failures and ensure that any failures are corrected during a period when no real emergency exists. CTIA strongly supports all of these efforts and encourages FEMA and other public-safety authorities to offer training opportunities for alert originators that promise to bolster WEA's utility and credibility going forward.

CTIA and our member companies are also keenly focused on the security of wireless networks. Wireless providers work in a collaborative partnership with network equipment manufacturers, chipset and device providers, and the application ecosystem to build robust security in and around wireless networks. They use a combination of technology, security best practices, innovative tools, and tight physical and virtual access controls to manage and protect their networks.[13] In our National emergency alert system, wireless providers participating in WEA depend on the integrity of the messages received from alert originators and FEMA. To promote our common goal of a trusted WEA system, CTIA and the wireless industry engage with the FCC, FEMA, and alert originators to share expertise in the identification of threats and development of recommendations.[14]

While we expect there are many lessons to be learned from the experience in Hawaii, and many will be cautionary, we should also acknowledge that wireless networks and devices performed exactly as designed and effectively delivered and presented the alert message as received from the FEMA gateway. The speed and effectiveness of its delivery should give policy makers and the public confidence that in the event of a real emergency, the Wireless Emergency Alert system will disseminate information rapidly and accurately to Americans—wherever they may be.

CTIA and the wireless industry are proud of the critical role that Wireless Emergency Alerts play in our Nation's emergency alert system, and are committed to continue working collaboratively with public safety professionals at every level of our Government to maintain system integrity and public confidence in Wireless Emergency Alerts.

Thank you for the opportunity to testify today. If CTIA can provide any additional information you would find helpful, please let us know.

Mr. DONOVAN. Thank you, Mr. Bergmann.

The Chair now recognizes Mr. Matheny for an opening statement.

STATEMENT OF SAM MATHENY, CHIEF TECHNOLOGY OFFICER, NATIONAL ASSOCIATION OF BROADCASTERS

Mr. MATHENY. Good morning, Chairman Donovan, Ranking Member Payne, and Members of the subcommittee. My name is Sam Matheny, and I am the chief technology officer at the National Association of Broadcasters.

On behalf of the thousands of free local television and radio broadcasters in your home towns, thank you for inviting me to testify on the emergency alert system, how broadcasters fulfill their role as first informers, and how innovation will allow broadcasters to do even more to keep viewers and listeners safe during emergencies.

Broadcasters take seriously their role as the most trusted source of news and emergency updates, whether it is preparing listeners and viewers for the coming storm, directing them to needed supplies and shelter during the disaster, or helping rebuild in the aftermath.

Local stations are part of the communities they serve. Broadcasting is sometimes the only available communications medium in

[13] CTIA, *Protecting America's Wireless Networks*, Apr. 2017, *https://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf.*

[14] See, e.g., FCC, *Communications Security, Reliability, and Interoperability Council V, Working Group 2, Emergency Alerting Platforms, WEA Security Sub-Working Group*, Final Report.

an emergency when wireless networks fail. Morning Consult recently found that the American people turn to broadcasters in times of emergency by a factor of more than 3 to 1.

Broadcasting is unique for the following reasons. First, broadcasting covers virtually everyone. Broadcast signals reach more of the U.S. population than any other communications medium.

Broadcasting is localized. Local broadcast stations can deliver market-specific information, as well as National alerts.

Broadcasting has no bottlenecks. An emergency alert can reach millions of people simultaneously without concern over network congestion.

Broadcasting is redundant. There are numerous independently operated stations in each market that deliver alerts.

Broadcasting is resilient. Stations often operate with backup equipment, generators, and fuel supplies to stay on the air.

Broadcaster information is actionable. Radio and television can provide enough information to enable people to understand what is happening and what steps they should take.

Finally, broadcasters are trusted. They are members of the local community and speak not just as an authority, but as a neighbor.

But broadcasters do more than just deliver messages to the public. Broadcasters are also the backbone of the emergency alert system. Working with the Government since the 1950's, broadcasters have operated and evolved a Nation-wide wireless network to deliver emergency alerts.

This daisy chain of broadcast stations ensures that emergency alerts can be delivered independent of Internet connectivity and even when power outages may disrupt other forms of communication.

In fact, broadcasters serve as primary entry points for emergency communications to the public and are thus part of the solution from beginning to end.

Because broadcasting plays such an important role in this critical communications infrastructure, it is vital that the Government support and foster broadcasting. I would like to briefly outline three key areas for your consideration.

First, broadcasters are in the final and most complicated phase of the incentive option, the repack phase. Nearly 1,000 television stations will be moving to new channel assignments and this will also impact over 700 FM radio stations on collocated towers.

Broadcasters need the time and money required to make these moves successfully and without impairing the public's ability to access emergency alerts. I ask for your support of the Viewer Protection Act and the Radio Consumer Protection Act and urge their passage as no station should be forced off the air due to lack of funds or unreasonable time constraints.

Second, broadcasters have been working with the wireless phone manufacturers and service providers on market-based solutions to activate the FM chips that are in smartphones. Our market efforts have been successful with one very notable exception, Apple.

We believe Apple should be encouraged to activate the FM tuner in future models of their iPhone as it will improve people's access to vital information in times of disaster.

Third, the next generation television standard, ATSC 3.0, which was recently approved by the FCC, has many features that will improve emergency alerting, including the ability to wake up sleeping television sets, more precise geotargeted alerts, and sending rich multimedia files such as weather radar images evacuation maps and even video files with detailed explanations of the emergency and what to do. New regulatory hurdles should not be placed in our way as we deploy next-gen TV.

In conclusion, in emergencies large and small, our Nation and your home towns benefit from a strong and vibrant broadcast industry. FEMA calls broadcasting a redundant, resilient, and necessary alerting pathway. I agree.

Thank you for having me here today, and I look forward to any questions you may have.

[The prepared statement of Mr. Matheny follows:]

PREPARED STATEMENT OF SAM MATHENY

FEBRUARY 6, 2018

INTRODUCTION

Good morning, Chairman Donovan, Ranking Member Payne, and Members of the subcommittee. My name is Sam Matheny and I am the chief technology officer at the National Association of Broadcasters (NAB). On behalf of the thousands of free, local television and radio broadcasters in your hometowns, thank you for inviting me to testify on the Emergency Alert System (EAS), how broadcasters fulfill their role as first informers and how innovation will allow broadcasters to do even more to keep viewers and listeners safe during emergencies. In addition to my role at NAB, I bring another perspective to these issues having spent nearly 20 years with Capitol Broadcasting Company, parent to WRAL–TV in Raleigh, North Carolina. There I worked directly with State emergency officials to help develop demonstrations of mobile alerts and warnings. Additionally, I have experience serving on committees that advise the Federal Communications Commission (FCC) and Federal Emergency Management Agency (FEMA) on a wide variety of network security, reliability, and public safety issues, and specifically on how to improve our Nation's Integrated Public Alert and Warning System (IPAWS).

BROADCASTERS' UNIQUE ROLE AND EXPERIENCE IN EMERGENCY ALERTING

As the most trusted source of news and emergency updates, Americans' first choice is to turn to local television and radio stations to get the information they need to keep safe during emergencies. Local stations are part of the communities they serve, and broadcasters do not hesitate to put themselves in harm's way to bring critical information to their neighbors. Whether it is preparing listeners and viewers for the coming storm, helping them access needed supplies and shelter during the disaster or helping towns and cities rebuild in the aftermath, local broadcasters take seriously their commitment to protect the public.

Recent fires and mudslides on the West Coast and hurricanes in Texas, Florida, and Puerto Rico have once again shined a bright light on our Nation's emergency preparedness and response abilities. While this is obviously true for first responders and all levels of government, it is also true for broadcasters. FCC Chairman Ajit Pai reminded us just last month that in times of crisis first responders and first informers work hand-in-hand, noting that "[b]roadcasting and public safety have been lifelong companions." While this sort of cooperation received National attention during the recent hurricanes and wildfires, it was just as true 2 years ago when over 60 tornados ravaged parts of 11 States across the southeast and just a few months later when quick and devastating floods overtook large parts of West Virginia and Virginia in what the National Weather Service (NWS) referred to as a One-Thousand-Year Event. In each of these cases and in countless others, broadcasters were there, serving their listeners, viewers, and communities.

Broadcasters invest heavily to ensure they remain on the air in times of disaster. Facilities often have redundant power sources, automatic fail-over processes, auxiliary transmission systems, generator back-up and substantial fuel reserves. Because of the strength of the broadcast infrastructure and the power of the airwaves, local

radio and TV stations are often the only available communications medium during disasters, even when cell phone and wireless networks can be unreliable. FEMA officials have noted that in times of emergency there is no more reliable source of information than local broadcasters. To give just one example, last year after Hurricane Maria moved through Puerto Rico and left much of the island without power and access to even basic information, not only were local television and radio stations continuing to provide life-saving alerts and information all throughout the ordeal, but afterward NAB partnered with numerous State broadcaster associations, FEMA and local officials in Puerto Rico to deliver 10,000 battery-powered radios to island residents who had no other lifeline.

This unique combination of trust and reliability is why, in addition to our on-going, comprehensive news coverage of emergencies, broadcasters form the backbone of the Emergency Alert System. We have all seen or heard the familiar announcement "The following is a test of the Emergency Alert System. This is only a test." EAS connects over-the-air broadcast radio, television, and cable systems, and is used during sudden, unpredictable, or unforeseen events. EAS participation is technically voluntary, yet virtually all radio and television stations participate, and do so proudly, even purchasing EAS equipment at their own expense. Today, the EAS, along with Wireless Emergency Alerts (WEAs) and National Oceanic and Atmospheric Administration (NOAA) Weather Radio, is part of the IPAWS umbrella, enabling State and local emergency managers to integrate with the National alert and warning infrastructure.

LESSONS LEARNED FROM NATION-WIDE EAS TEST AND RECENT EVENTS

In September 2017, FEMA, in coordination with the FCC and the NWS, conducted a Nation-wide test of the reliability and effectiveness of the EAS. Generally, the results of the test were positive, as a majority of EAS participants received and retransmitted the message, and participation improved compared to a previous test in 2016.

However, as the residents of and visitors to Hawaii know all too well after last month's false alert of a nuclear attack, our Nation's public alert and warning system and the emergency managers that originate messages are not always perfect. In an instant, one emergency manager's mouse click triggered a local and National panic, compounded by a lack of information and delay in disseminating correct information via official channels. Several items arising out of this unfortunate incident are worth discussing.

First, the most important takeaway is that the EAS system worked; radio and television broadcasters were on the case. The mistaken EAS alert was immediately relayed by broadcasters, who verified the source of the message but must rely on emergency managers for validation of the emergency. Broadcasters also stood by to disseminate the All-Clear message. Unfortunately, it took emergency managers 38 minutes to issue the needed follow-up EAS message. In the mean time, broadcasters used other means to confirm and report that it was a false alarm as soon as possible. The EAS system is a critical part of the trust that people place in broadcasters during an emergency, but human error in the issuance of EAS alerts can impair that trust. Going forward, NAB hopes to work with all the relevant stakeholders to minimize, if not eliminate, any vulnerabilities in the EAS process that may hinder broadcasters from carrying out their duty as first informers.

Second, broadcasters support the continued implementation by FEMA of the IPAWS Modernization Act, legislation this committee helped author and pass in 2016. This legislation recognized that the continued success of EAS will depend on the expertise and ability of local authorities to fully and effectively deploy it. Broadcasters applaud FEMA's on-going efforts to train State and local authorities on the proper use of the system, and support this legislative effort to incentivize State and local officials to participate in training. Especially after Hawaii, it is more important than ever that local emergency managers know exactly how and when to trigger an EAS alert.

Third, Congress and the FCC should consider whether current WEAs provided by the wireless industry are sufficient to adequately alert and warn recipients in times of emergency. Twenty years after the pager was supplanted by the brick phone, then the flip phone and now the smartphone, a WEA delivers text-only emergency information to recipients, often with fewer characters than a tweet. Often, these alerts simply direct recipients to "check local media." A multi-stakeholder FCC advisory committee that I served on recommended that WEA be improved by increasing the number of characters from 90 to 360 so the alerts would be more informative and useful. Further, this committee also recommended that WEA include embedded links and phone numbers so recipients could quickly gain access to additional infor-

mation. These suggested enhancements were opposed by the wireless industry before the FCC, but were ultimately authorized in September 2016 and are awaiting implementation. In contrast, I will detail below several ways in which radio and television broadcasters are innovating to better inform their communities when it matters most.

POLICY CHOICES CRITICAL TO BROADCASTERS' CURRENT AND FUTURE CAPABILITIES

It is important that Congress be mindful of several policy choices that will enable broadcasters to continue and improve upon this important emergency role.

Next Generation TV

Broadcasters are pleased that the FCC recently approved a joint petition of the NAB, Consumer Technology Association, America's Public Television Stations and the Advanced Warning and Response Network Alliance, requesting permission for stations and television receiver manufacturers to voluntarily adopt the world's first Internet Protocol (IP)-based terrestrial television transmission standard, ATSC 3.0, also known as Next Gen TV. Not only will Next Gen TV allow broadcasters to deliver sharp ultra HD images, multichannel immersive sound, interactive features and customizable content, but more importantly it will enable an even more effective distribution of information to the public during disasters and in times of crisis.

With the advanced alerting capabilities of Next Gen TV, a television broadcaster will be able to simultaneously deliver geo-targeted, rich-media alerts to an unlimited number of enabled fixed, mobile, and handheld devices across their entire coverage area. For example, and at the consumer's discretion, rather than simply running an EAS alert or crawl over regularly scheduled broadcast programming for an entire market's viewing audience (and then only reaching those who are watching), a Next Gen TV signal could wake up enabled devices and reach the entire universe of devices within its television signal contour. Using the rich-media capabilities of Next Gen TV, broadcasters can provide targeted neighborhood-specific alerts that include text, graphics (such as Doppler radar animations or an evacuation route), pictures, and even detailed video-on-demand descriptions. The public will have access to all of this actionable, life-saving information even if the power goes out or cellular wireless networks fail.

As broadcasters, we are simply planning to use our spectrum licenses more efficiently and to better serve our viewers. We are not asking for any additional spectrum, Government funds, or mandates. Unlike other communications providers, broadcasters are the only licensees that must ask the FCC for permission to innovate with regard to our transmission standard. However, by adopting Next Gen TV, broadcasters will have much greater flexibility to innovate going forward. As long as new regulatory hurdles are not placed in our way, more and more viewers across the country will benefit from these innovations and the advanced emergency alerting systems that Next Gen TV will enable.

Spectrum Incentive Auction Repack

While broadcasters are innovating for the future, there are also near-term obstacles that without action could prevent emergency alerts from reaching local broadcast viewers and listeners. I'm referring to relocating—or repacking—nearly 1,000 broadcast television stations in the final and most complicated phase of the broadcast spectrum incentive auction. Additionally, in the process of full-power television stations moving frequencies, this will also negatively impact more than 700 FM radio stations and countless low-power television and translator stations that are critical to bringing service to rural America. Quite simply, if a television or radio station is forced off the air for any period of time due to circumstances outside of their control, it will diminish the ability of the public to receive critical EAS information.

FCC Chairman Pai testified before Congress in July that the funds originally set aside to reimburse broadcasters for relocating are woefully inadequate. Not only does this funding shortfall violate Congress' promise to hold broadcasters harmless but, in some cases, the shortfall is actually preventing stations from making the advanced purchases required to complete their moves in a timely fashion. In fact, according to the most recent quarterly status reports filed with the FCC, 11 percent of stations changing channels are already behind, despite their best efforts to complete their moves. Accordingly, NAB supports legislation such as the Viewer Protection Act (H.R. 3347) and Radio Consumer Protection Act (H.R. 3685), and urge Congressional passage to ensure that your constituents do not lose access to local television and radio stations during these mandated frequency moves due to a lack of funds or unreasonable time constraints.

FM Chip Activation

The radio broadcast industry has continued to take a leading role in ensuring that a life-saving technology is available to millions of Americans through their smartphones. Over the past several years, broadcasters developed marketplace partnerships with wireless phone manufacturers and providers to turn on—or at least not deactivate—FM receivers that are already installed in devices. This endeavor has grown exponentially over the past few years and, with one notable exception—Apple's iPhone, many Americans are able to access FM radio through their smartphones during times of emergency, even when the cellular network may be down due to congestion or physical damage.

CONCLUSION

In conclusion, I would like to thank you again for having me here today to speak about the critical role that broadcasters play in the Emergency Alert System and ensuring the public's safety. This is a mission our industry takes very seriously and we have a track record of fulfilling. We look forward to working with Congress, State, and local governments and other industry partners to strengthen the entire system going forward. I look forward to answering any questions you may have.

Mr. DONOVAN. Thank you, Mr. Matheny.

The subcommittee now stands in recess subject to the call of the Chair. We will reconvene right after votes. Thank you.

[Recess.]

Mr. DONOVAN. I thank the witnesses for their opening statements. I now recognize myself for 5 minutes for questioning.

Mr. Krakauer, I wanted to ask you about New York City issuing a wireless emergency alert during the Chelsea bombing, which you talked about your opening statement.

How effective was the tool for New York City and in our public service agencies?

Mr. KRAKAUER. So I think it was a very effective tool. Our first two messages were highly targeted to a several-square-block area in the Chelsea neighborhood.

The first message was at the request of NYPD directing people in the area to shelter in place when that secondary device was discovered. Then the second message went to the same area and directed people to shelter in place order had been lifted, because the bomb squad from NYPD successfully contained that device.

The challenge we saw with that message is even though we highly geotargeted it to the Chelsea neighborhood, we received anecdotal reports from other parts of Manhattan, other boroughs, one case in New Jersey. So people far outside that target area did receive that message.

That concerns us from a warning fatigue perspective. People who receive messages that are not aimed for them or not intended for them are more likely to opt-out of the system, which is why we have been, you know, encouraged by the FCC's latest rules and working with industry on improving geotargeting.

The city-wide message that went out the following Monday looking for the suspect ultimately led to his capture, so that was a very successful message. Would have been more successful, however, if we were able to embed an image in that message as opposed to indicating the public should go to the media to see the picture.

Mr. DONOVAN. Right. As you know, I live in New York City as well. We are unique compared to some other geographic areas of our country because we have subways.

Do you find difficulties? Are the alerts effective in the subways? I forget how many millions of riders we have every day. Because

of our subway system, that is also a target for potential terrorist attacks. Do you find that the alert system is adequate in the uniqueness of trying to push those messages out to people who might be riding on our subways?

Mr. KRAKAUER. So right now, you know, if you are able to get wireless service in your device, which is the case in most subway stations, you should receive the WEA message. The challenging part would be if you are in between stations where there is not wireless service yet, particularly from the networks, I know that the MTA is working on improving that.

That said, we are in touch on a regular basis through our emergency operations center watch command with the rail control center, so if we do need to get a message to the MTA, we talk to them directly dozens of times a day about lots of incidents.

Mr. DONOVAN. Mr. Bergmann, can you talk about industry's capabilities in, you know, making sure that uniqueness of New York City subway riders are protected as well as the people who are above ground?

Mr. BERGMANN. So thank you, Mr. Chairman. Certainly happy to, and, you know, we continue in the wireless industry to be very supportive of the wireless emergency alert program, recognizing the important role that it plays.

You talked a little bit about the importance of that, that it played in the Chelsea bombing. In response to that, we are continuing to do things to make it even stronger by improving the geotargeting, by building in that ability to access embedded links so that you can get those kinds of pictures and actionable information. So that is very much a focus for us.

Then in terms of coverage, our Members I know have worked closely with the subway authorities and have wireless service now in, I think, all 284 of the stations in Manhattan, Queens, and the Bronx.

You know, as Mr. Krakauer said that challenge is inside the tunnels and getting access to the tunnels, you know, when the trains run, you know, 24/7, to make sure that you can deploy there.

But wireless infrastructure siting is one of our top priorities. Making sure that we can build our infrastructure out there, to make sure that we get as much coverage and as much capacity as possible, is one of our top priorities in the wireless industry.

Mr. DONOVAN. Thank you. In my last minute, could you talk a little bit about, right now, I could send you a photograph of my 2½-year-old daughter. Mr. Krakauer can't shoot out a photograph of the Chelsea bomber. What are the obstacles in, you know, are we going to be able to overcome those?

Mr. BERGMANN. Sure. So we have certainly strengthened our capability with ability to send an embedded link so that you can get that picture. Sending it in the message involves additional capabilities.

Part of the way we built WEA is using a different technology. It is called cell broadcast technology. We did that so that we could make sure that we get the message to as many people as possible as quickly as possible. We are talking within seconds, not within minutes.

That is different than a typical text message that you and I might send, and if I sent it to three people in this room, you might get the text message right away and somebody else might get it 5 minutes or an hour later. We want to make sure that message gets there immediately. So that has really been the focus and the priority.

Mr. DONOVAN. My limited understanding, because my VCR still flashes 12 back home, is that, and you have to tell some of the younger people in the audience what a VCR is. But it is the less amount of data in the message will get it out quicker, the more complicated the data is, or the more space that it will take up, the slower the message delivery is?

Mr. BERGMANN. I think you put your finger on it, and I would think about it in two ways. One is the technology was built using this this cell broadcast technology that wasn't built to incorporate that multimedia, so that is an additional capability that we have to build out.

The second piece is just making sure that we are being cognizant of congestion on networks. If we are looking to send out a message to 8½ million people in New York City then we want to make sure that then those networks are available to contact public safety or to contact their loved ones in the case of an emergency.

Mr. DONOVAN. Since we only have two other Members to ask questions, I am going to take the liberty to ask you one more. Are we able to overcome...or are our alerts able to take priority in messages, as you are saying the system might be clogged with people sending texts to one another, are our alerts able to take priority over non-emergency messages?

Mr. BERGMANN. That is exactly right. That is why we built this specific technology to make sure that wireless emergency alerts get there quickly.

Mr. DONOVAN. Thank you very much.

The Chair now recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

Mr. Gaynor and Mr. Krakauer, in the days following the false alert in Hawaii last month, we realize that we don't necessarily train for mistakes. How are you adjusting your training and exercise policies to ensure that people working for you understand what to do if a false alert does go out?

Mr. GAYNOR. Thank you, Mr. Payne. We have a generally robust training exercise program within the agency and with our central partners. This is an opportunity to look at, unfortunately, an unfortunate incident in Hawaii and take advantage of those lessons learned, and apply them to your jurisdiction. So we have gone back to square one.

We have has those people that are assigned to actually make these systems work, have the authority to do it, actually monitor how it is done, make sure they know how to do it, make sure that if there is a shortfall in understanding of the system, and there are many systems that we rely on, that they know how to do it. It is readily available. You know, time is of the essence when these things happen.

So we have really doubled down on making sure that we really, truly understand the systems, so the hardware, all those things that go into it, and really the function of the system, because this requires a human in the chain.

With a human in the chain, there are going to be some difficulties with making mistakes. I think the best way to avoid mistakes or increase that time is that you have to touch it. You have to do it. You have to do it for real. You just can't read about it in a book.

So we are all about training and exercise to make sure we can do it, should you ask us in, you know, in a minute or in, you know, a month or in a year. We want to be able to do it for all flawlessly and seamlessly.

Mr. PAYNE. Your training is germane to Rhode Island. With what they are doing in Hawaii, would probably you all have different policies and training, or is there an overall guide to what you should be working on?

Mr. GAYNOR. So I think when it comes to, you know, how we interact with the Federal systems, we prescribe to the Federal training, Federal exercise and procedures and policy. Every State is unique in how they apply that to their jurisdiction.

I am unfamiliar with the exact protocols that Hawaii had. I would imagine that many of these protocols and policies are similar throughout the United States.

But again, I am going to take a guess that every State has a unique protocol that they follow. It is up to us as State directors to make sure that it is right-sized for your State, right-sized for the hazards that you deal with on a daily basis, and making sure the public understands when that message goes out it is for real.

Mr. PAYNE. OK, thank you.

Mr. Krakauer.

Mr. KRAKAUER. Thank you, sir. So with respect to training, our public warning team trains on a weekly basis. We call it WEA Wednesday in New York City. Every Wednesday, the public warning team is required to send out a test message.

It does not go all the way out to the public. We use FEMA's testing system, and wait for the acknowledgment codes back from IPAWS.

With respect to policies and procedures, we view WEA as a two-person job in New York City, both during training and during live emergency operations.

There is a public warning specialist who is on the keys entering that message, filling out the form to make sure we hit all the checkboxes and get all the information necessary so that it does go out to the public when an emergency is happening. Standing right behind them is an on-duty supervisor who is making sure that policy and procedure is being followed to the letter.

Those trainings are custom to the software applications that we have in New York City, which are going to be different than they have in Rhode Island or different than they have in Hawaii.

There is not one software system that integrates with FEMA's system. It is up to local jurisdictions what they ultimately purchase.

Mr. PAYNE. OK. For you gentlemen, once again, alerts and warnings are used to warn the public of both natural and man-made

disasters. When an alert goes out, is it important that the follow-up advice Government entities issue is consistent?

Can you talk about how you coordinate public messaging among relevant State and local agencies in neighboring jurisdictions when appropriate after an initial emergency alert goes out?

Mr. KRAKAUER. Sure. So in New York City once we issue an alert, you know, a lot of our neighboring jurisdictions also received those alerts, either through the IPAWS system or through our own distribution list.

Another system that we have developed is something called the Regional Emergency Liaison Team Route, and that is the neighboring jurisdictions and emergency managers. It is actually a protocol that New York State institutes.

You know, soon after, or leading up to an emergency, we all get on a conference call and share what our individual jurisdictions are doing, what our message is, and act as consistently as possible.

Mr. PAYNE. OK, thank you.

Mr. Gaynor.

Mr. GAYNOR. The State, we have a policy called the State Emergency Notification Policy that has all major stakeholders involved. There are certain processes and protocols that we use in that, and it is similar to New York.

I think the first thing we do with key decision makers is we have a conference call, whether that is on a telephone or on HSIN depending on what the subject matter is and then multiple groups within our State system called Code Red, communities that we can notify.

So whether it is local emergency managers, or it is hospitals or it is all of them together, with some fidelity, we can tailor that message and get it to those groups pretty quickly.

Mr. PAYNE. OK, thank you.

Mr. Chair, I yield back.

Mr. DONOVAN. The gentleman yields.

The Chair recognizes the gentleman from Rhode Island, who was kind enough to invite Mr. Gaynor to be a member of our panel, Mr. Langevin.

Mr. LANGEVIN. Well, thank you, Mr. Chairman. I want to thank you and the Ranking Member for holding this hearing here today, and I want to thank our panel of witnesses, thank you for your testimony.

I particularly want to extend a personal welcome to our director of EMA, Peter Gaynor, who is doing, in my estimation in every measure, an excellent job as our director. It is an honor to have you here today.

Let me start out with Mr. Gaynor and ask him if there is anything else you wanted to add. Again, I understand that the RIEMA has used its State-wide system Code Red and also IPAWS to issue alert warnings as to Rhode Islanders about severe weather events.

Any further description you would like to offer in terms of experience with that system to describe RIEMA's use of your alerting system and the importance of original alerts and warnings to the citizens of Rhode Island?

Mr. GAYNOR. Thank you, Congressman, for inviting me today. It is a pleasure to be here. Again, looking at what has happened

across the country, what happened today, or what happened in Hawaii, we want to take advantage of this opportunity never to let a crisis go really unused, so we want to take advantage of that.

I have a particular interest now to understand not only systems like WEA and EAS, but really how all these systems are strung together in a scenario.

So whether FEMA is announcing some sort of indicational warning over the National alert system NAWAS, what does that really mean for a State? What actions are they asking us to do? What actions are FEMA doing on behalf of the State? How do we interact and how do we get that right down to the lowest level?

So as a State director, I am kinda in the middle between the Federal Government and I am talking about a major catastrophic event, you know, how do you, you know, meld those two worlds together to make sure you save time, you get a clear concise message to everyone that is affected so they can take proactive protective measures to save themselves, their families and their community?

Mr. LANGEVIN. Thank you. Thank you.

Again, to you, Mr. Gaynor, and it is certainly our witnesses are also welcome to comment. But obviously cybersecurity risk remains one of the risks that Rhode Island and probably most of the States is least prepared to mitigate, given the challenges associated with it.

How could an incident targeting our emergency management systems, including alerts and warning systems, affect your agency's ability to operate?

Mr. GAYNOR. I think it is everyone's worst nightmare that you cannot use these systems that we rely on every day. You know, the cell phone is, you know, everyone has one, it is how we communicate.

The question that I have been asked by my staff, my fellow directors in New England and others is, you know, what happens if we cannot communicate via these things that operate perfectly in a blue-sky scenario?

How do you actually take those alert warnings and get them down to the local taxpayer or resident in your community? How do you do that? I am not sure I have the answer. I think one of the gentleman up here is the backbone of how we do it now is the radio system and that is it.

But should the radio system fail, what is next? I think we probably have to take a deeper look into that. I think cyber is a threat that is here to stay. It is touching every system that we build, and we probably have to take a real hard look about if all that fails what are we going to do.

Mr. LANGEVIN. Sure, good points, and it is one of my worst-case scenarios, too, and things that keep me up at night as well.

Let me turn to Mr. Bergmann and Mr. Matheny. While the alert in Hawaii last month originated from an authorized sender, alert disseminators like broadcasters and wireless providers are not immune, certainly, from unauthorized use of warning systems.

This was demonstrated in 2013 when pranksters actually hacked the emergency alert systems of local broadcasters in at least two States and issued false alerts about an impending zombie apoca-

lypse. Obviously these alerts were swiftly debunked, but the potential remains to severely undermine trust in the system.

So to that point, you know, what are the members of your organizations doing to secure alert systems like EAS or WEA and the new ATSC 3.0 standard from unauthorized access including by cyber beings? Anything you want to comment there?

Mr. MATHENY. Sure, I will. It is OK? I will start. We certainly take cybersecurity very seriously and as an organization we have been working with our members and we have formed a cybersecurity task force. This is a group of CIOs and chief information security officers that meet regularly to share best practices.

We have also had numerous seminars and webinars educating our members on good practices. We have a member portal that we have set up that has access to different resources and we are in the process of developing a more extensive educational program.

We really encourage the use of the NIST framework, which really plays on a lot of things around, let us refer to a cyber hygiene, the idea of managing your passwords in a correct way, of setting up your equipment around and behind appropriately configured firewalls and protected networks, as well as who has physical access to the equipment.

So we are working quite diligently to make sure that folks are engaged on cybersecurity and creating the most secure as possible systems.

Mr. BERGMANN. Thank you, Congressman. For the wireless industry, security is amongst our highest priorities. So we are very focused on protecting against cybersecurity threats and I would really say on a 24/7/365 basis.

We know that those threats continue to evolve, but our members are very, very focused on it in terms of their everyday practices, the equipment they deploy, the practices that they use, the personnel, and they also embrace the NIST cybersecurity framework as well, too, and have worked within CTIA.

We have a cybersecurity working group that convenes 30 members to share best practices, to share information. They are very oriented around risk assessment and risk management so we work together to try to address those issues. We also work closely with our partners in the Federal Government as well, too.

We worked closely with the FCC's CSRIC Advisory Committee to look at threats to the alerting systems. Of course, coordinate very closely with our partners at DHS on a daily basis to try to make sure that we are assessing and appropriately responding to any threats.

Mr. LANGEVIN. Very good. Well, my time has expired, but I want to thank all of our witnesses for testifying here today. Thank you for your insight and your input and for the job you are doing to keep people safe. Thank you.

I yield back the balance of my time.

Mr. DONOVAN. Gentleman yields. Because you came all the way here and your expertise is so valuable to us, we each want to ask one more question. This committee has always had action items after our hearings. We don't just gather testimony, we actually do something with the information that you provide us with.

So to everyone on the panel, I would just like to ask, what would you like to see this committee do? Whether it be in the area of emergency management responding, whether it be in the area of wireless or in broadcasting, what could this committee do to help you to protect the citizens of this Nation, better than we are already protecting them? Mr. Matheny.

Mr. MATHENY. Sure, thank you very much. I think if I had one ask to make it would be to ask for your support of the Viewer Protection Act. As I mentioned earlier, we are in the process of the repack.

We have got over 1,000 TV stations moving, 700 radio stations that are going to be impacted and in the context of what we are talking about today, those are all emergency alert providers. They are all part of this system and we cannot afford to have any of them taken off-line because of time line that is unreasonable or because of lack of funding.

Chairman Pai has testified that there is a significant shortfall in funding and we also believe that, probably to the tune of about $1 billion. So we would love to see support for the Viewer Protection Act.

Mr. DONOVAN. Thank you, sir.

Mr. Bergmann.

Mr. BERGMANN. Mr. Chairman, I would highlight three things for you. The first is Congress has a unique role in making more spectrum available for use by the wireless industry and that is really key to increasing capacity.

The second is Congress also plays a key role in terms of promoting infrastructure deployment. So we talked a little bit about coverage earlier. By enabling the wireless industry to build out that next generation of wireless networks, which is based on small cells, we can again increase that ability to target those messages.

Last, I think we are all interested and invested in making sure that we are exchanging best practices, that alert originators have access to all of the information about the tools that are available, and so working together to promote those kinds of best practices would help as well.

Mr. DONOVAN. Thank you very much.

Mr. Gaynor.

Mr. GAYNOR. I will go back to my training exercise theme. I think in the past we have tested systems to see if the systems worked, can you get that message from point A to point B, and I think that is important. So I would like to see more scenario-based alert warning training and exercises.

Again, you can do it for a State, you can do it for a region, you can do it for the country and pick a scenario that is applicable and run that through the entire course, right?

Make sure it works from beginning to end, through all the systems and prove that you can get that message out should a local, State, or Federal Government need to do it. So again, more realistic training I think is what I would like to see.

Mr. DONOVAN. Thank you, sir.

Mr. Krakauer.

Mr. KRAKAUER. Mr. Chairman, I would highlight two things. The first, you know, we thank you and the Members of the sub-

committee for your continued support of the Urban Areas Security Initiative and preserving that money.

We think in light of today's threats it is very important that that money continue not to just be preserved, but increased in lots of areas, but certainly in terms of public warning.

The other thing I would note to the committee is that the situation in Hawaii highlighted a good question for us as local emergency managers is, are State and local governments the right avenue to respond to a National threat from a state actor?

We think that the Federal Government should look at making that a Federal responsibility as part of whether it is FEMA or the Homeland Security or the Department of Defense, the Federal Government really is in the best position to detect a threat from a State actor and issue warnings initially to the general public.

Time is of the essence and, you know, State and local authorities are not really in the best position to make those notifications.

Mr. DONOVAN. I thank you all for your testimony, your candid answers to my questions and the rest of the panel. I want to thank each of you for your dedication, commitment to the safety of our Nation. Chair now recognizes Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

Mr. Bergmann, as you know, mobile customers are able to opt-out of most WEA alerts.

As I mentioned in my opening statement, I am concerned that the false alerts and alert fatigue could in fact lead to people to opt out of WEA alerts. Today, Mr. Krakauer suggested that Congress eliminate the opt-out option. Does CTIA agree?

Mr. BERGMANN. So thanks, Mr. Congressman. So you are exactly correct. Today consumers are able to opt out of amber alerts and imminent threat alerts, but not Presidential alerts and that is part of the Warning Act.

I think from our perspective, you know, we would defer to policy makers on the appropriateness of opt-in versus opt-out. I think we would like to see consumers use wireless emergency alerts. We recognize that they want access by their wireless device and they recognize how valuable that is.

So our goal has been to try to make sure we do everything that we can to minimize alerting fatigue and to make sure that the system has trust and confidence and we will do everything that we can to execute on that.

Mr. PAYNE. OK. In the mean time, what are your members doing to educate customers on the value of the warnings and alerts?

Mr. BERGMANN. Sure, so we certainly work closely with the FCC, with FEMA, in terms of education efforts. We have done a PSA at CTIA to try to let folks know about it.

I think the good news is that you have subscribers representing 99 percent of the overall U.S. subscribership that get their service from a wireless provider who voluntarily participates in WEA.

Mr. PAYNE. OK, well I thank you, all of you for being here, for your testimony. It has been very valuable. As the Chairman said that we will be using this information to craft legislation in the future. So with that I yield back.

Mr. DONOVAN. Gentleman yields. Thank you, Mr. Payne.

The Chair recognizes—nope. The Chair recognized that Mr. Langevin has left. I want to thank all witnesses for their valuable testimony and the Members of my committee for their insightful questions.

The Members of the subcommittee may have additional questions for the witnesses and we will ask you to respond to those in writing. Pursuant to committee rule VII(D) the hearing record will remain open for 10 days. Without objection, the committee stands adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]